UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. ROMAN SELEZNEV, Defendant.	CASE NO. CR11-70RAJ SEATTLE, WASHINGTON June 2, 2016 EVIDENTIARY HEARING Vol. 2 of 2

VERBATIM REPORT OF PROCEEDINGS
BEFORE THE HONORABLE RICHARD A. JONES
UNITED STATES DISTRICT JUDGE

APPEARANCES:

For the Plaintiff:
NORMAN BARBOSA
SETH WILKINSON
HAROLD CHUN
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101

For the Defendant:
JOHN HENRY BROWNE
EMMA SCANLAN
Law Offices of John Henry Brown
108 S Washington Street
Seattle, WA 98104

Reported by:
NANCY L. BAUER, CCR, RPR
Federal Court Reporter
700 Stewart Street, Suite 17205
Seattle, WA 98101
(206) 370-8506
nancy_bauer@wawd.uscourts.gov

EXAMINATION INDEX

EXHIBIT INDEX

June 2, 2016 9:36 a.m.

PROCEEDINGS

THE CLERK: We are here in the matter of United States v. Roman Seleznev, Cause No. CR11-70, assigned to this court.

If counsel and the interpreters could please rise and make your appearances for the record.

MR. BARBOSA: Good morning, Your Honor. Norman Barbosa and Harold Chun on behalf of the United States.

MR. BROWNE: Good morning, Your Honor. John Henry Browne and Emma Scanlan for the defendant.

THE COURT: Counsel, your next witness.

MR. BARBOSA: The government calls Special Agent Michael Fischlin.

Before we start, Your Honor, I will inform the court, we have turned over additional exhibits to the defense last night, and we showed them one additional exhibit we had this morning. They're still being printed for the witness and court's copy, as well as the defense copy. With the exception of one new exhibit, those are exhibits for a later witness and we believe to have them in everyone's binders before the witness takes the stand.

THE COURT: All right. Please step forward.

MICHAEL FISCHLIN, HAVING BEEN FIRST DULY SWORN, TESTIFIED AS FOLLOWS:

THE CLERK: Please state your first and last name, and spelling your last name for the record, please.

THE WITNESS: My name is Michael Fischlin. Last name is spelled F-i-s-c-h-l-i-n.

THE COURT: Sir, if you'll get closer to the microphone.

THE WITNESS: Yes, sir.

THE COURT: You may inquire.

DIRECT EXAMINATION

BY MR. BARBOSA:

Q Where are you employed?

A I'm employed by the Secret Service currently in the Seattle field office.

Q How long have you been employed by the United States Secret Service?

A Approximately 14 years.

Q When were you assigned to the Seattle field office?

A In September of 2008.

Q What are your duties with the Secret Service in Seattle?

A Well, duties are twofold. One, we have a protective mission, so I help support protection for the President, vice president, and other protectees of the Secret Service. Also investigate threats against those individuals.

And then, in addition, we investigate a large variety of financial crimes and even cybercrimes.

Q What types of cases are you typically assigned to in terms of an investigation?
A Since I'm a member of the Secret Service Seattle field office Electronic Crimes Task Force. I typically investigate electronic crimes such as cybercrimes.
Q How long have you been a member of the Electronic Crimes Task Force?
A Since April of 2011.
Q What kind of training did you receive to do your work as a member of the Electronic Crimes Task Force?
A I completed a variety of forensic training. I completed the Basic Computer Evidence Recovery Training course at the Federal Law Enforcement Training Center. I completed the Advanced Computer Evidence Recovery Training course at the Cyber Crimes Center. I completed the Point of Sale Investigations course done by Trustwave at the Secret Service Training Center. I completed the Basic Mobile Device Examination course by the Secret Service at the University of Tulsa, and some other courses.
Q What has your work entailed since becoming a member of the Electronic Crimes Task Force?
A Well, twofold. Part of my duties will be examining electronic media, being such as computers, hard drives from computers, and mobile devices, and then also investigating electronic crimes.

Q Approximately how many examinations have you conducted?
A Approximately 530.
Q What type of devices have you examined?
A Computers. Mainly computers running Windows-based operating systems. Hard drives in computers. Flash media and mobile devices, such as mobile phones, GPS units, tablets.
Q Turning to United States v. Seleznev, how did you first become involved in this case?
A I was assigned the case in February of 2014.
Q And what do you mean by "assigned the case"?
A Well, the previous case agent, Special Agent Kirk Arthur, was promoted. And, as a result, he had to relocate to another office, so I was assigned that case when he left.
Q What was the status of the investigation when you were assigned?
A It was an open case. But, at that point in time, we were waiting for an opportunity to identify where the subject was located and apprehend him.
Q And the "subject" being Mr. Seleznev?
A Correct.
Q Was there an arrest warrant issued for him at that time?
A There was.
Q When you were assigned the case, what actions did you take in furtherance of the investigation or efforts to capture

Mr. Seleznev?

A At that point in time, none.

Q Between February of 2014 and July of 2014, do you recall any activity on this case?

A One piece of information I received from the Secret Service Cyber Intelligence Section, in approximately May of 2014, was they believed the defendant was running the dump shop, 2pac.cc.

Q Did you do anything with that information?

A I did not.

Q What did you do to familiarize yourself with the investigation, if anything, at that point in time?

A At that point in time I didn't do anything.

Q What were you doing during that period of time?

A Sure. Well, I was working a variety of my own cases. And, also, I was heavily involved in conducting forensic examines of electronic media for other agents in the office, as well as other local agencies. That took up a lot of my time. And, finally, I helped our protection mission traveling for the President and vice president and others.

Q Do you know when this investigation had started?

A I believe it was approximately August of 2010.

Q And do you know who the original investigating agent was?

A Yes, in Seattle it was Detective David Dunn.

Q What was Detective Dunn doing in 2014 when you were

assigned to this case?
A He had moved on to the private sector, new employment.
Q Do you recall approximately when he had left?
A Approximately, early 2013.
Q And when this investigation started in 2010, were you a member of the Electronic Crimes Task Force?
A No.
Q Drawing your attention to early July 2014, did you learn of an opportunity to arrest Mr. Seleznev?
A Yes.
Q How did you first learn about that opportunity?
A It was on June 30th, 2014, our Cyber Intelligence Section advised that they believed the defendant was in the Maldives vacationing, and they were going to try to reach out to the local authority to see if it was possible to apprehend him.
Q Did you become active in the case at that point?
A I was requested for documents on the case, and I provided those.
Q Who was handling the planning of the operation?
A Secret Service Cyber Intelligence Section.
Q What, if anything, did you do to prepare for the arrest?
A I was providing document. And I knew, ultimately, if he was apprehended and if there was any evidence, that it would make its way to Seattle since we are the controlling field office.

Q Did you begin to review the file?
A I reviewed it from requested documents such as the indictment warrant. I was asked if there was a Red Notice in place. I learned one had been completed but had not been turned in. So I provided a copy of the application that had been filled out that hadn't been submitted.
Q Approximately how many days passed between receiving notice that there might be an opportunity to arrest Mr. Seleznev and the operation to arrest him?
A Approximately four to five days.
Q Was that a busy time period?
A Very.
Q Do you know what the file consisted of, approximately how large of a file this was?
A It consisted of investigative reports, search warrant affidavits, some forensic examination results, subpoenas, a wide range of information.
Q What was the volume of this material?
A It was a lot.
Q When you say "a lot," do you mean a few reports?
A Several years' worth of reports, various search warrant affidavits, various subpoenas. So it was a lot of data.
Q Had evidence been gathered as a part of the investigation?
A Yes.
Q What was the volume and nature of the evidence?

A Forensic examinations of electronic media and those reports, search warrant returns, media. There was a variety of areas where evidence had been gathered.
Q Did you have time to review all this material?
A No.
Q Did you participate personally in the arrest operation in the Maldives?
A No.
Q Do you know who participated in that?
A Yes.
Q Was Agent Iacovetti one of those?
A Yes.
Q After Mr. Seleznev was arrested, did you learn that a laptop computer had been seized from him?
A Yes.
Q Was that computer brought to Seattle?
A It was.
Q Do you know who brought it to Seattle?
A Yes, Special Agent in Charge David Iacovetti.
Q When did it arrive in Seattle?
A Approximately 5:30 in the morning on July 8, 2014.
Q How long after his arrest was that?
A A few days.
Q Did you see the computer when it arrived?
A Not initially.

Q When did you first see it?
A Well, after transporting Special Agent in Charge Iacovetti from the SeaTac Airport to the Seattle field office, we went up to the main conference room in the Seattle field office and laid out the evidence in the conference room. So that was the first time I saw it.
Q Where was it -- how was it carried when you first saw it?
A It was in a blue bag, which I was told was obtained from the defendant.
Q And was it taken out of the blue bag when it arrived in the office?
A Yes.
Q What was done with it after being taken out of that blue bag?
A Well, the evidence was laid out, and then we're going to inventory it on permanent inventory forms. Special Agent in Charge Iacovetti had put it -- inventoried the items on a temporary handwritten evidence form. So we were putting it on a permanent form identifying make, model, and serial number.
Q Showing you what has been admitted already as Government's Exhibit 4. Do you recognize this?
A Yes.
Q Is this the first page of that inventory form that you're referring to?

A Yes.
Q Turning to the fourth page of the Exhibit 4, you referenced a handwritten inventory; is that right?
A Correct.
Q Is this that handwritten inventory?
A It is.
Q So what did you do in relation to the computer and confirming the inventory?
A Well, verify the make, model, and serial numbers, and recorded those on the permanent inventory form.
Q The serial number was written on the handwritten inventory, correct?
A Yes.
Q Why did you verify it?
A It's practice.
Q The typewritten forms that are pages 1 and 2 of this inventory, who created those?
A I did.
Q I'm now showing you Government's Exhibit 2. Do you recognize that?
A I do.
Q What is it?
A It is an access log for the main evidence vault at the Seattle Secret Service field office.
Q How is this relevant to the computer?

A Well, it shows that on July 8, 2014, that the evidence was added to the main evidence vault.

MR. BARBOSA: Government offers Exhibit 2.

THE COURT: Any objection?

MS. SCANLAN: No objection.

THE COURT: It is admitted.

(Exhibit 2 admitted.)

Q (By Mr. Barbosa) Why did you check this into the main evidence vault?

A That would be common practice when we receive evidence.

Q And who signed this main evidence vault log?

A Our office manager, Aline Rolfe.

Q Where is it reflected on this form that this computer was added to the main evidence vault?

A It is reflected under the column, Evidence added or removed from vault," and then handwritten there is "added" and then a serial number, and that would be the entry for the electronic evidence entering the vault.

Q Which line is that?

A It is line 2.

Q Is that the line I've highlighted here?

A Yes.

Q Where is the main evidence vault located?

A It is within the Secret Service Seattle field office.

Q Is the Secret Service Seattle field office secured in any

fashion from outside access?
A Yes, it is, in multiple ways.
Q Without disclosing any security measures that might be sensitive, where is that?
A Well, it's alarmed, for one. There's ballistic doors and then there's various other things you have to do to enter the vault.
Q Who has access to the main evidence vault?
A It's limited to supervisors and our administrative officer and then maybe one other admin that has access, but agents generally do not have access to the main vault.
Q Is the main vault secured in any fashion?
A Yes, it is.
Q How is it secured?
A Alarmed. And then it's also deadbolted, combo locked, cyberlocks. There's multiple, multiple ways.
Q Did you go into the main evidence vault?
A I don't recall going in the main evidence vault on that day.
Q The following day, did you move the computer to a different evidence vault?
A Yes.
Q Why did you move it to another evidence vault?
A In preparation. I expected that we'd get a search warrant for electronic media in the near future. So I moved it to

our electronic crimes evidence vault in the Seattle field office, so they'd have access to it when they obtained the warrants.

Q Turning attention back to Exhibit 2. Where is it documented that the computer was removed from the main evidence vault and moved to the other evidence vault?

A On the third line, July 9, 2014, it shows that the vault was opened. However, our admin did not place an entry for the evidence leaving the vault on the access log.

Q Should that have been done?

A Yes.

Q When you say "the vault was opened," you mentioned earlier that the vault is secured with locks. When this reflects the vault has opened, are those locks -- is there free access to the vault?

A No. It is still secured.

Q What does it mean to be opened then?

A Less that you have to do to enter it. It's still secured but not in as many ways. For example, the alarm would be off when the vault is opened, but the access mechanism is required to enter it.

Q Is the move from the main evidence vault to the ECTF vault reflected on any other form?

A Yes, the chain of custody.

Q Where on the chain of custody form?

A It should be on the back page.
Q Page 3 of Exhibit 4, is that what you mean by the back page?
A Correct.
Q Where does this reflect?
A It would be line 3.
Q Could you read that?
A Yes. "Items 1 through 5, on July 9, 2014, to SA Fischlin for ECTF exam by hand, and there is my signature."
Q So what is the ECTF evidence vault?
A It is a vault for temporary storage of electronic items to be examined.
Q Where is that vault located?
A In the Seattle field office of the Secret Service, at the other end of the hall from where the main evidence vault is.
Q Is it behind the same controlled entries and exits?
A Yes.
Q Who has access to the ECTF evidence vault?
A Supervisors, administrative personnel. And then for regular agents at that time, it was just myself and Special Agent Mills.
Q How is that evidence vault secured?
A In the same way as the main evidence vault.
Q An alarm and a lock?
A Yes.

Q Do you maintain a separate vault log for the ECTF vault?
A Yes.
Q Showing you what's been marked as Government's Exhibit 3. Do you recognize that?
A Yes.
Q How do you recognize that?
A It is the access log for the ECTF evidence vault.
MR. BARBOSA: Government offers Exhibit 3.
MR. CHUN: No objection.
MS. SCANLAN: No objection.
THE COURT: Admitted.
(Exhibit 3 admitted.)
Q (By Mr. Barbosa) Does this show the entry of the computer into the ECTF evidence vault?
A Yes.
Q Where?
A On the final line.
Q Is that where I've focused in on now?
A Yes.
Q Who signed the log that day?
A I put my name on it. I didn't sign it.
Q Okay. Was anyone else with you that day?
A Yes.
Q Does this log require everyone who enters the vault to sign?

A The form does say that, but it's not office practice.
Q Why isn't it office practice?
A I don't know. It's just not what's ever occurred, to my knowledge, while I've been in the Seattle field office.
Q What did you and Agent Mills do with the computer that day?
A We inventoried electronic evidence into our ECTF evidence vault.
Q What did inventorying it into the vault entail?
A While redundant, we verified make, model, and serial number, and then affixed a unique label to each device. For example, 14-108, that label was affixed to the Sony Vaio laptop; meaning, in calendar year 2014, it was the 108th electronic device added to that specific vault.
Q During that process, did you notice anything unusual?
A During the process, the splash screen on the laptop had come on.
Q What do you mean by "splash screen"?
A Looked like a rainbow-type color.
Q What did you do? How did you react when the splash screen came on?
A Well, I remember telling Special Agent Mills to make a note of that.
Q Do you know why it displayed?
A It had to have some form of power.

Q Did you turn the computer off after that?
A No.
Q Why not?
A For one, we didn't have a search warrant. And we really believed that, due to the nature of the case and the defendant, that the device would be encrypted. And if it were encrypted, we'd want the opportunity to potentially capture random access memory. Because in random access memory, we could potentially get encryption keys to decrypt the disk.
Q Why did you think it would be encrypted?
A Well, for one, the nature of the case being a cyber case, a hacking case, we believed there was a strong likelihood the device would be encrypted.

And, also, I received a message from one of the agents in Guam when the device was there. He indicated that there was a sticker on the laptop saying Windows 8 was installed and that BitLocker, by default, was installed on that version of Windows. So that is a form of encryption that we believe may have been running on the device.
Q So you needed power to be on the device?
A You need power to potentially capture RAM. Once it is powered off, the RAM is lost.
Q Was the device plugged in at that point?
A It wasn't.

Q Why didn't you plug it in?
A I believed we'd be getting a warrant in the near future.
Q Did you get a warrant soon thereafter?
A No.
Q Did you document the fact that the screen displayed?
A Special Agent Mills did.
Q Okay. Let's go back to the splash screen. I'm going to show you what's been marked as Government's Exhibit 5. Do you recognize this?
A Yes.
Q How do you recognize this?
A A photo taken by Special Agent Mills, an example of a splash screen on Windows 8.
Q And does that appear similar to the splash screen that you saw on July 9th?
A Yes.
Q Is it the same splash screen?
A It appears to be the same type.
Q Is it written in English?
A No. But it appeared to be the same type of splash screen in a rainbow color. This is in English.
Q Is this computer in the photograph, Mr. Seleznev's computer?
A It is not.
Q What is it?

A It is -- it is a Sony Vaio similar model, but a different model with the Windows 8 installed on it.
Q The splash screen you saw, did it display in English?
A Not that I recall.
Q Do you recall it displaying any written characters?
A No.
Q Do you recall it displaying a password hint?
A No.

MR. BARBOSA: Government offers Exhibit 5.

THE COURT: Any objection?

MS. SCANLAN: Your Honor, this appears to be, I would say, for illustrative purposes only, since it is not the computer and it is not the splash screen.

MR. BARBOSA: Correct.

THE COURT: Okay. It is admitted for illustrative purposes.

(Exhibit 5 admitted.)

Q (By Mr. Barbosa) This computer, you were aware it was a Windows 8 machine. Is that what you just said?
A Yes.
Q Did you have any reason to believe this was a cellular-enabled device?
A I did not.
Q Did you have any reason to believe that it could connect to a wireless network without user input?

A I did not.
Q Did you place it in a Faraday bag?
A No.
Q Why didn't you place it in a Faraday bag?
A To my knowledge, it was not a cellular device that could connect to a tower. And, to my knowledge, the device would not connect to an unknown network without user interaction.
Q Were you concerned that it could possibly connect to a network without any input?
A I wasn't.
Q Why weren't you concerned about that?
A I didn't feel it was something that would have happened.
Q Had you had training on this type of protection, use of a Faraday bag?
A Yes, for mobile devices.
Q Did you consider this a mobile device?
A I considered it a laptop computer, not a mobile device.
Q So after checking this in on July 9th, did you begin preparing a search warrant to search this laptop?
A Yes.
Q How soon after the arrest did you begin to prepare that warrant?
A I believe I started on or about July 8th.
Q When did you first send a draft of that warrant to me at the U.S. Attorney's Office?

A July 10, 2014.
Q And July 9th was what day -- sorry. July 8th was what day of the week?
A I think a Tuesday.
Q Okay. And July 10th would have been Thursday, then?
A Yes.
Q Okay. Was I the AUSA assigned to work with you in July of 2014?
A Yes.
Q Do you know who the original AUSA was back when this case was?
A Yes, AUSA Kathryn Warma.
Q Do you know whether she was still working at the U.S. Attorney's Office in July of 2014?
A She was retired.
Q Do you know when she retired approximately?
A I don't.
Q Were you also helping to prepare for Mr. Seleznev's identity hearing in Guam at that time?
A I was.
Q What did that involve?
A Involved trying to learn as much as I could about the case by reviewing the case files, so I was fairly familiar with it for testimony at the identity hearing. Included getting exhibits that were requested for that identity hearing, and

more.

Q Did you have to review the evidence in detail to prepare that hearing?

A To the best that I could.

Q What type of evidence did you have to review?

A Investigative reports, search warrant affidavits, forensic examination results.

Q For the identity hearing, what were you trying to learn about in order to testify?

A Identity information from the investigation that indicated we had the right guy, that this was the correct Roman Seleznev that was wanted in the case.

Q What type of evidence review did that entail?

A It included looking at forensic examination results where his name had been found, travel -- travel documentation, his name on servers in the case, pulling documents that were obtained from him when he was apprehended for exhibits, and just reviewing the case file in general to be familiar with the case.

Q How much back and forth with the U.S. Attorney's Office in Seattle did that involve?

A A lot. It was daily.

Q Did that also involve interaction with the U.S. Attorney's Office in Guam?

A It did.

Q Was there a significant time difference between here and Guam?
A Yes.
Q Approximately how many hours, do you recall?
A I know they are approximately a day ahead of us.
Q Did this affect your work on the case?
A Yes.
Q How?
A Well, it required quick responses to information being wanted, so -- and I knew.
Q Was that at normal hours of the day?
A No.
Q So after sending the first draft to my office on Thursday the 10th, when did you receive comments and suggestions back from me?
A That was July 16th, 2014.
Q Did those comments and suggestions require you to conduct additional research in order to continue working on the draft?
A Yes.
Q What type of continued research did you have to conduct?
A Again, reviewing the case file, locating exhibits that were requested, and also preparing for travel to Guam because I now knew I was going.
Q That additional research that you had to conduct for the

search warrant, who were you working with and who were you consulting with during that time period?

A Detective David Dunn, and also our Cyber Intelligence Section provided information since they had made the link between the defendant and the 2Pac domain.

Q Was that an easy set of evidence to understand?

A No, it was complex.

Q What did you have to do to begin understanding it?

A I had to review the case file, information provided by the other agents, so I got a decent understanding of it for affidavit preparation.

Q Did some of that information include financial records?

A Yes. Liberty Reserve, I remember in particular.

Q Who produced those?

A That was our Cyber Intelligence Section.

Q What was the volume of that data?

A It was -- I can't remember the volume. I remember it was pretty complex due to the way they linked the defendant to various Liberty Reserve accounts and various email addresses and ultimately to the 2Pac nickname.

Q Did you come to understand it eventually?

A Generally. It is still quite complicated.

Q What is Liberty Reserve?

A It was a form of e-commerce or digital currency.

Q Okay. After receiving comments and suggestions back from

me on the 16th, did you have to leave the United States for business?

A I did. I had to fly to Guam on July 19th, 2014, for the identity hearing in the case.

Q When did you say you had to leave?

A It was July 19th, 2014.

Q Was that on a weekend?

A It was on a Saturday.

Q And when was the hearing in Guam supposed to take place originally?

A On or about July 22nd, 2014.

Q So when did you expect to return?

A A day or two after that.

Q Did the hearing actually take place on July 22nd?

A No.

Q Why not?

A It was postponed numerous times due to defense motions and also on one day due to bad weather.

Q Despite being in Guam for the identity hearing, did you continue to work on the affidavit?

A Yes.

Q When did you send another draft back to Seattle?

A I believe I sent my final draft on July 22nd, 2014.

Q At that time did you still expect to be back in Seattle shortly?

A Yes.
Q When did the hearing in Guam finally take place?
A It concluded on July 31st, 2014.
Q At some point during the week of July 21st while you were in Guam, did you receive an offer of assistance from another agent in DC to fill in for you on this warrant?
A Yes.
Q Who offered the assist?
A Special Agent Richard LaTulip.
Q Why did he offer to assist?
A Because I was in Guam for identity hearing.
Q Is it typical to receive assistance like this to swear out a warrant for you?
A No.
Q Why did you -- I'll withdraw that.
You're the case agent assigned to this investigation, correct?
A Correct.
Q And you've sat through the testimony here yesterday?
A Yes, I did.
Q I'd like to turn to another topic.
MR. BARBOSA: I'm providing the court and defense counsel with Exhibit 53, which I've already shown to counsel.
Q (By Mr. Barbosa) You heard defense experts' testimony that someone logged on to the computer on July 7th, didn't

you?
A I did.
Q Do you recall when they said somebody had logged on to the computer?
A July 7th, 2014.
Q And did they list a particular -- an exact time for that?
A Yes.
Q Do you recall when that was?
A Approximately 19:47.
Q Okay. You also heard Agent Iacovetti's testimony?
A I did.
Q And do you recall seeing the Exhibit 28 that has been admitted, his airline ticket?
A Yes.
Q When did he depart Guam?
A 6:25 a.m.
Q On what day?
A That was July 8th, 2014.
Q Yesterday after the hearing, did you convert this time to UTC time?
A Yes.
Q Showing you what's been marked as Government's Exhibit 53. Do you recognize this?
A Yes.
Q What is this?

A It shows time zone conversion between Guam and the UTC with the conversion.

MR. BARBOSA: Government offers 53.

MS. SCANLAN: No objection?

THE COURT: Admitted.

(Exhibit 53 admitted.)

Q (By Mr. Barbosa) Converted to UTC, when did Agent Iacovetti leave Guam?

A Converted UTC was approximately 6:30.

Q You can read it in military time. That's fine.

A All right. In UTC was 20:25 UTC time, on July 7th, 2014.

Q How is that in relation to the time that the defendant alleged a logon had occurred?

A It was approximately 30 minutes later.

Q That he departed Guam?

A Correct.

MR. BARBOSA: No further questions, Your Honor.

THE COURT: Cross-examination?

CROSS-EXAMINATION

BY MS. SCANLAN:

Q Good morning.

A Good morning.

Q So you were assigned the case in February of 2014; is that right?

A Yes.

Q So in July of 2014, you were not new to the case?
A No. I had it for a little bit of time.
Q How many months is that, four or five?
A Approximately.
Q So let's talk about the serial number on the Sony Vaio. Okay?
Agent Iacovetti arrives on July 8th, correct?
A Yes.
Q And he and you lay out all of the items in the main conference room?
A Yes.
Q You take the evidence log. He has the temporary evidence log that he's filled out with the serial number, correct?
A Correct.
Q Do you verify that onto the permanent log by looking at the Sony Vaio?
A Correct.
Q At the time when you observed the Sony Vaio, I assume the screen was facing up?
A I can't recall what way the screen was facing.
Q Doesn't the screen only face one way?
A It can face up, but you can turn the device and see the bottom of it.
Q You mean you don't remember if was like this?
A When we first laid it out? When we first laid the device

out?
Q No. Just the time you were in the conference room.
A I don't recall what way it was facing initially.
Q Do you recall ever seeing the screen up the entire time that you were in the conference room?
A I'm sure that it did.
Q Because this particular laptop, right, the screen is on top? It's not underneath when you shut it, right? It doesn't face the keys?
A Correct.
Q It only faces up?
A Yes.
Q Where is the serial number located on the laptop?
A It is located on the backside of it.
Q So, then, the laptop and this other stuff was checked into the main evidence vault; is that correct?
A Yes.
Q And the administer is the only person who assigns evidence in and out of that vault?
A Correct.
Q But your vault, the task force vault, has numerous people that can sign in and out?
A We have a few more that can, correct.
Q Are both those vaults in the same office?
A They are.

Q And that office it takes up, what, one floor, half a floor?
A Yeah, three-quarters of a floor, half.
Q But you needed to move it out of the main vault into your own vault the day after it got there?
A I did.
Q So you went in, moving to July 9th, right?
A Yes.
Q You go into the -- is it the ECTF, that's the acronym, right?
A Yes.
Q You go into the ECTF vault with Agent Mills?
A Yes.
Q How long were you in the vault?
A Approximately 20 minutes.
Q Okay. This is the vault log, right?
A It is.
THE COURT: Exhibit number, counsel?
MS. SCANLAN: Sorry, Your Honor. Exhibit No 3.
Q (By Ms. Scanlan) What is this time of entry over here on the left, July 9th, 2014, at 09:31?
A Yes.
Q That's 9:31 a.m.?
A It is.
Q And you leave at 15:53?

A Yep.
Q What time is that?
A 3:53 p.m.
Q I don't get that. You were in there for 20 minutes?
A Yes.
Q What were you doing the rest of this six- or seven-hour period between when you entered and when you exited?
A On that specific day, I can't remember, but the vault was closed. It just remains -- it's unalarmed, so you can go in and out during the course of the day until the completion of the day. So you secure it completely at the end of the day, which is what the 3:53 p.m. would note.
Q Okay. So at 9:31 a.m., you go into the vault with Agent Mills, right?
A Yes. That's when it was opened for the day.
Q And you guys were in there for approximately 20 minutes?
A Approximately.
Q And when you leave, you didn't sign out?
A No.
Q And Agent Mills did not sign in when he entered?
A He didn't.
Q And he did not sign out when he left?
A No.
Q Is that an acceptable practice within the Secret Service?
A Yes. That's not the -- the purpose of the form, for

office practice, would show when the vault was open, the time it was open. And, at the conclusion of the day, the time the vault was secured and who closed it.

Q So part of this form about everybody signing it is superfluous to what you're supposed to do?

A It's not office practice for everyone to sign it.

Q How long have you been a Secret Service agent?

A I've been with the agency for 14 years, been an agent for approximately eight years.

Q And you've had training on chain-of-custody issues?

A Yes.

Q Chain of custody is one of the reasons that people sign in and out of a vault, right?

A Well, the chain of custody was completed on the device. The log is separate from the chain of custody.

Q So what is the purpose of the log?

A To show when evidence was ultimately added to the vault and when evidence ultimately left the vault.

Q So the vault and the vault log has nothing to do with documenting who has access to the evidence and what time and what day?

A It would show who brought it into the vault.

Q But it doesn't matter who accesses it once it's there?

A Well, there would be restricted access to it, to that vault.

Q But based on this log, we can't really recreate who had access to it when; is that right?
A On who specifically, after that timeframe, took possession of the device?
Q No. Who had access to it during this time period.
A It would be limited to people with access to that particular vault.
Q What is the difference between the vault being secured and unsecured?
A Secured for the day, so it would be alarmed. There would be a cyberlock on it and a combo lock. When it's not secured for the day, it would be unalarmed, but you still have to get through a locking mechanism such as a cyberlock. So it's closed and secured, but not as secured as it is at the end of the day where it's also alarmed.
Q So if you decided to go in and out of that vault during that time period 20 times, we're not going to know that from this log?
A Correct.
Q So on July 9th when you guys are in the vault, the serial number of the Sony Vaio has already been documented on paper twice, right?
A It had.
Q And you're aware that Agent Mills is saying that he woke up the splash screen, because he was looking for the serial

number?
A I'm aware of that.
Q You sign off on Agent Mills' reports, right?
A I don't sign off on his reports.
Q You don't?
A I don't do -- I guess, can you elaborate on that question?
Q I can.
So his report -- his initial report, I haven't seen a date on it, but it says it's requested by you, and he does it?
A I'm the requester, yes. I was the requester for that.
Q Who is the reviewer?
A The reviewer, the Secret Service has a peer-review program. So I don't know who the peer reviewer was for that particular report. It was not me.
Q Does the reviewer -- like crime labs and stuff, the reviewer would sign off on the report on a document. Is it the same practice for the Secret Service?
A Well, the general report, not all the attachments, would be reviewed in another system. And then that peer reviewer would ultimately have to provide any feedback, if they had any, before they click the approve button. I was not the peer reviewer on that report.
Q Are you aware the initial report does not indicate that the splash screen turned on on July 9th?

A No.
Q Are you aware the supplemental report does not indicate that?
A No.
Q But you asked Agent Mills. You put him in charge of documenting that that computer turned on, right?
A I asked him to make a note of that.
Q What was the purpose of the note?
A The purpose of the note was, it was -- we knew that it had some sort of power when it came to life. And we knew when it had come to life at that moment, there may have been some changes made to the device. So I wanted him to be able to document that date and time to explain some activity that may have appeared on that drive during his examination.
Q So before that, though, Agent Iacovetti had told you that the computer turned on when he had it on the plane, right?
A He told me that he had seen the splash screen at some point.
Q Was it important to document that fact?
A It would have been, yeah.
Q Is that in your report?
A No. I wasn't the handler.
Q Okay. You were aware, it appears that there was a Windows 8.1 Pro sticker on this laptop. Somebody from Guam told you that?

A That there was a Windows 8 sticker of some sort on it, yes.
Q Who told you that?
A Special Agent Scott Lam.
Q And who is Scott Lam in all of this?
A He is an agent out of our Los Angeles field office. He's also trained in forensics. And I know that he was on the ground in Guam after the defendant had arrived there at some point.
Q So he was on the ground in Guam. Did he tell you that he handled or looked at the laptop to know the sticker was on it?
A He sent an email that said he saw a sticker on the outside of the laptop, yes.
Q So he saw the laptop, I suppose, at some point when it was in Agent Iacovetti's custody?
A I assume so.
Q I'm sorry, you said that -- is it Lam?
A Yes, L-a-m.
Q Agent Lam has training in computer forensics; is that correct?
A Yes.
Q So at the time Agent Lam notified you, hey, this is potentially a Windows 8 machine, you knew that Windows 8 had some kind of -- what was it called? Bit...

A A BitLocker was installed.
Q What is a BitLocker?
A BitLocker provides full-disk encryption, if enabled. It's by Microsoft.
Q So that's a pretty specific piece of information about Windows 8, yeah?
A Sure.
Q But you didn't know that Windows 8 had Connected Standby?
A I didn't.
Q When you found out it was a Windows 8 machine, which was before it even got there, right?
A Yes.
Q Did you research Windows 8?
A No.
Q The BitLocker piece was something you already knew?
A Yes.
Q What else did you know about Windows 8?
A It was a fairly new operating system.
Q That's it? It's fairly new, and you happen to know it has BitLocker on it?
A Yes. BitLocker was around before that, but I believe by default it was installed at that point on Windows 8 operating systems.
Q Let's go back -- and I apologize, this isn't in grouping. But I want to go back to the July 9th vault access, okay?

A Yes.
Q So it turns on, and you're aware obviously that it has some kind of power?
A Yes.
Q It's not plugged in in the vault, I'm assuming?
A It wasn't.
Q And did you observe it turn off, the splash screen?
A Yes. At some point it did turn off.
Q How long was it on?
A I can't recall. I know it wasn't very long. A few minutes, tops.
Q Did you tell Agent Mills to make a note of how long the screen was on?
A No. Just the date and time that we observed it.
Q So at some point it turns off. And is this when you and Agent Mills have a conversation about doing a Live RAM Capturer?
A When it -- either then or shortly after, we talked about the possibility that that may be something that would be done.
Q While you were still in the vault or after you left?
A I can't recall if it was right then or shortly after.
Q But you didn't plug it in?
A We didn't.
Q And you didn't turn it off?

A We did not.
Q How do you handle a tablet? If that was a tablet in this vault and the screen came on, what would you do?
A I would have done the same thing at that point.
Q Most tablets, like phones, right -- I'm going to use the wrong word. But they have some sort of connection capability?
A Depends. Some tablets have built-in cellular capabilities, but many do not. And, as a result, they rely on a Wi-Fi to be able to connect to a network.
Q So even though you knew that some tablets have this -- what is it? Say it again, network...
A Cellular capability.
Q Cellular capability, thank you. You would have done nothing different had that been a tablet?
A At that point in time, if it were on -- can you rephrase the question?
Q Yes.
The Sony Vaio is referred to by Agent Mills as a hybrid laptop tablet, right?
A Yes.
Q And it has this unique configuration where the screen is up, unlike other laptops, right?
A Right.
Q So it's in the vault. So my question is: If you were in

that vault and Agent Mills is doing whatever he is doing with that device, and that is a tablet and it turned on, what would you do?

A If I knew it had cellular capabilities, I would have brought it into our lab, which is right around the corner, and put it into a shielded test enclosure, which is a Faraday box. But if it wasn't, if I did not know it had cellular capability, I would have done nothing. I would have left it where it was.

Q So if this was a tablet and you didn't know, you would just assume that it didn't have that capability?

A From my experience as an examiner, most of the devices I've come across, tablets have not actually had cellular capability. I think I've only actually dealt with one. However, I know they can have that functionality. So unless I knew it had that capability, I would not have done anything differently.

Q Tablets, now that I think about it, when you have an iPad and you have like Verizon, you can buy a cellular plan for your tablet, right?

A Some you can.

Q You didn't --

MS. SCANLAN: I'm sorry? May I have one moment?

THE COURT: Yes.

MR. BROWNE: Sorry, Your Honor.

MS. SCANLAN: I don't remember what we were talking about.

THE COURT: Your next question, counsel.

Q (By Ms. Scanlan) At the time that you had the Sony Vaio in the vault, you did not know whether it had connectivity ability or not, right?

A I did not believe it had cellular capability. It appeared to me to be a laptop computer.

Q Did you work on the iPad in this case?

A No. It was Detective Hansen.

Q Do you know if he worked on it within a Faraday box?

A I think when he brought it into the lab, at that point he did.

Q But if it had been you, you would not have done that?

A Are we talking about upon me examining it or inventorying it into the vault?

Q Inventorying it.

A Inventorying it, no.

Q What if it had turned on?

A If it had turned on, I knew it had cellular capabilities, absolutely put it in an enclosure. But without that, with it turning on, I would not have worried about it.

Q Let's talk about the time between when the laptop came into your office's custody and the warrant. So you testified that you were very busy during that time period, correct?

A Yes.
Q How many agents are employed, approximately, by the Secret Service?
A Approximately, my guess is 3,500.
Q So you were not the only person available to work on this warrant, I'm assuming?
A I was the case agent.
Q I know, but were you the only available agent?
A To work on that warrant?
Q Yes.
A Yes, the case agent to work on the warrant. I don't know who else would have done it.
Q But that's not quite what I'm asking. I'm asking, were you the only person available?
A In my opinion, yes.
Q Did you check with LaTulip at some point during this 23-day period to see if he was available?
A During the -- I know, on or about July 10, 2014, he started to offer assistance in some investigation.
Q And did you take him up on that?
A Yes.
Q July 10th?
A Approximately.
Q But you did not have him help you with the warrant?
A No. I was available and preparing it. I'd actually

submitted one that day, and affidavit of my rough draft.
Q And you got it back from Mr. Barbosa six days later?
A Yes, July 16th.
Q At what point did you become concerned enough to have someone else work on the affidavit, or swear it?
A When I was in Guam.
Q When you were in Guam -- there's a field office there, right?
A Yes.
Q Somebody testified about that. It has regular Internet access and those sorts of things?
A Yes.
Q After you left the Sony Vaio on on July 9th, did you think about whether it was going to lose power during that next 23-day period?
A I honestly did not.
Q On July 30th, did Agent Mills tell you that it had powered off?
A Can you restate that? I'm sorry.
Q Yes. On July 30th, when Agent Mills removed it, did he tell you that it had powered off?
A I don't think so.
Q When did you become aware of that fact?
A I think after I got back from Guam in early August.
Q Did you tell Agent Mills to put in his report that it was

off when he took it out on July 30th?
A I didn't tell him either way to do that or not do that.
THE COURT: Counsel, we're at 10:30. Is this a good time to take a break?
MS. SCANLAN: Yes, Your Honor.
THE COURT: We'll be in recess.
(COURT IN RECESS.)
THE COURT: Good morning. Please be seated. Counsel, you may inquire.
Q (By Ms. Scanlan) When the laptop came in on July 8th, did it have a bottle cap over the power button?
A I don't remember the bottle cap. I do remember myself and Special Agent in Charge Iacovetti discussing it, though.
Q And you heard them talk about it yesterday?
A Yes. And I remember that we talked about it. I can't vividly remember the bottle cap itself.
Q So, then, I'm assuming you didn't keep it?
A No.
Q This email that Agent Lam sent you, what in total did it say about the laptop?
A Gave a make, model, serial number, and then a subsequent email that had a sticker on it indicating there was a version of Windows 8 installed, and that he believed that BitLocker encryption was installed on that version of operating system.
Q This Sony Vaio has an external port for a mobile SIM card,

right?
A Not to my knowledge. It may, but not to my knowledge.
Q What is a mobile SIM card?
A A mobile SIM card would provide the device with the capability to connect to a cellular network.
Q And a computer that has a slot for that, it's like a cell phone, right? It has a little area where you put the thing?
A Yes.
Q So, then, I'm assuming you didn't look on the 9th to see if it had this capability, a little port for the mobile SIM card, right?
A Correct. I didn't know it existed.
Q You didn't know that it was possible for a computer to have a mobile SIM card slot?
A For a laptop at that time, no.
Q In general, how do you know when you receive a laptop into evidence whether it's on or not?
A You would know if you saw it come to life. Otherwise, I assume it is off. That's traditionally how they come into evidence.
Q I assume some laptops, when they're seized, are on?
A It happens.
Q And are the case agents in the field turning them off before they come to you?
A It depends on what happens in the field. Typically, there

is a forensic agent that goes out that assists with search warrants and seizing devices, and they'll deal with those matters on scene, not at the office.

Q So like Agent Lam being in Guam?

A Like somebody being there for the actual apprehension and immediately dealing with the devices, preparing them for -- securing them and preparing them for transportation.

Q So, generally, when you secure a laptop at the scene, you turn it off, right?

A No.

Q You generally leave it on?

A Generally, at this -- due to technology changing and as things are today, you would not turn it off. You try to collect volatile data before manipulating it. At that point after collecting volatile data, depending on the device, you may remove a battery, for example, but you want to collect volatile data, if possible, now.

Q So when you do it now, do you put the laptop in a Faraday enclosure of some sort?

A The laptop? No.

Q Even though it may be able to connect, like a tablet or a phone?

A Correct.

MS. SCANLAN: I have nothing further.

THE COURT: Redirect?

REDIRECT EXAMINATION

BY MR. BARBOSA:

Q Turning back to the ECTF vault. Ms. Scanlan suggested that numerous people had access to that. Is that true?

A Approximately five people have access to that vault.

Q And to get in, what do they have to do?

A They have to disable the alarm, if they're the first one entering for the day. They have to have a combo for the combo lock. And then they have to have their own code for a cyberlock.

Q Once it's opened for the day, do they still have to have a code for the cyberlock?

A Yes.

Q Were you with Agent Mills when he checked the serial number on July 9th?

A I was in the vault with him, yes.

Q Did you see him check for the serial number?

A Yes.

Q Did he, in fact, check for the serial number?

A He did. He was reading off the digits to me for me to confirm that they were accurate on the inventory form I completed the day before.

Q Is that when the splash screen displayed?

A Yes.

Q You asked him to make a note?

A I did.
Q Do you know if he actually made a note?
A Yes, he did.
Q Have you seen that note?
A I've seen it, yes.
Q Have you ever dealt with a laptop or tablet that would automatically connect to a network that had not previously been trusted?
A No.
Q Does this laptop, to your knowledge, have cellular capability?
A No.
Q You mentioned there are approximately 3,500 Secret Service agents?
A That's my guess.
Q Are they all in Seattle?
A No.
Q How many are in Seattle?
A Approximately ten.
Q How many are on the ECTF?
A Two.

MR. BARBOSA: I have no further questions.

MS. SCANLAN: I have no further questions.

THE COURT: Any objection to this witness being excused?

MR. BARBOSA: No, Your Honor.

THE COURT: Counsel for the defense?

MS. SCANLAN: No, Your Honor.

THE COURT: You may step down.

You may call your next witness.

MR. CHUN: The United States calls Special Agent David Mills.

DAVID MILLS, HAVING BEEN FIRST DULY SWORN, TESTIFIED AS FOLLOWS:

THE CLERK: Please state your first and last name, and spelling your last name for the record.

THE WITNESS: David Mills, M-i-l-l-s.

THE COURT: You may inquire.

DIRECT EXAMINATION

BY MR. CHUN:

Q Special Agent Mills, how are you employed?

A I'm a Special Agent with the U.S. Secret Service.

Q How long have you been with the Secret Service?

A Sixteen years.

Q And how about the Seattle field office, specifically?

A I've been at the Seattle field office since July of 2011.

Q And where are you currently assigned?

A I'm currently assigned to the Electronic Device Task Force.

Q And, as a Special Agent, what training have you received?

A I received, initially, special agent or Criminal Investigative Training at the Federal Law Enforcement Training Center in Glynco, Georgia, as well as more protective-related training at our facility in Baltimore, Maryland, for a total of about six months.

Q Have you received on-the-job training throughout the course of your career?

A Yes.

Q Now, as an agent assigned to the Electronic Crimes Task Force here in Seattle, what are your duties?

A I perform computer imaging, computer forensics, and computer examines.

Q And what training have you received for those, for computer forensics?

A I received, initially, the Basic Computer Evidence Recovery Training at the Federal Law Enforcement Training Center in Glynco, Georgia. I've also received the Advanced Computer Evidence Retrieval -- or Recovery Training in Fairfax, Virginia, at the DSHS facility there. I've received Network and Server Forensics Training, as well as Mobile Device Forensics Training.

Q And do you receive regular, like, ongoing training?

A Yeah. We have yearly in-service training.

Q In this case, United States v. Seleznev, 11-00070, how did you first become involved?

A I was requested to perform a computer-forensic exam on the defendant's laptop.
Q And when was that?
A That was in July of 2014.
Q And what training have you received -- sorry, this is duplicative -- of creating a forensic image?
A So the initial training at the Basic Computer Evidence Recovery Training, I received in 2012. We reviewed basic computer architecture, and also the imaging of computer hardware, write blockers, et cetera, write blocking and imaging computers.
Q When was the very first time you saw the laptop you were supposed to image in this case?
A I saw that device on July 9th, I believe the date was, of 2014.
Q And where was that?
A That was in our field office, as Agent Fischlin brought it into our task force evidence vault.
Q Was anyone else in that vault with you besides Agent Fischlin?
A No.
Q As you enter the vault, is there a log you sign into?
A Yes.
Q And showing you what's been marked as Exhibit 3, do you recognize this?

A Yes.
Q What is it?
A This is our vault security access log that's posted on the door of the vault.
Q And highlighted here, do you see the entry for July 9, 2014?
A Yes.
Q Whose name is there?
A That is Agent Fischlin.
Q Did you sign in that day?
A No, I did not.
Q Why not?
A It's office practice for the agent that initially opens the vault to sign in and do it that way.
Q Okay. So the office practice is even if two people go in, only one person signs?
MS. SCANLAN: Objection; leading.
THE COURT: It is leading, counsel.
Q (By Mr. Chun) Could you repeat the practice again?
A The office practice is for the initial person that opens the vault, at any given time of the day, to sign in with his name and the date and time, and anyone else coming in would just enter the vault.
Q Now, when you're inside this vault with Agent Fischlin, what did you do?

A At that time we were just making sure the device was placed in the vault correctly. We verified its identifiers, serial number and part number, and checked those with the documentation that was provided on the evidence forms that accompanied the device.

Q As you were documenting these items, did anything occur with the laptop?

A Yes. While I was attempting to identify the serial number, moving the device around, the screen did come on.

Q And what was on that screen?

A I call it a Windows splash screen. It just displays multicolored rainbows and the time and date.

Q Showing you what's been previously admitted as Government's Exhibit 5. What do you see here?

A That's the example of the Windows splash screen that I saw.

Q So it looks something like this?

A Correct.

Q After the screen turned on, what did you do?

A At that point I -- we continued to make sure we inventoried the device. We just left it and kept it in the -- on the shelf that it was on.

Q And what was your reaction to the screen turning on?

A Initially, it was kind of surprised that it was still on.

Q Did you say you were surprised?

A Yeah.
Q And did you record what you saw that day?
A Yeah. I entered it into my personal notes.
Q Showing you what's been marked as Government's Exhibit 10. Do you recognize that?
A Yes.
Q What is that?
A Those are my personal notes for the case.
Q So these are notes that you created?
A Yes.

MR. CHUN: Your Honor, move to admit Government's Exhibit 10.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 10 admitted.)

Q (By Mr. Chun) And on Government's Exhibit 10, do you see anywhere where you recorded seeing that screen turn on?
A Yeah. The top of the page in the entry for July 9th, the second line.
Q Could you just read that for us, please?
A Sure. "At approximately June 09," I think that's "38:00," "while locating the serial number for Item No. 14-108, Sony Vaio laptop, the unit's screen turned on and I observed."
Q And when did you record that?
A That was just within minutes after we put the device into

the ECTF vault.

Q How long were you in the vault on July 9th?

A I'd say no more than five to ten minutes, within that time range. Just enough to make sure it was there.

Q And what did you do after recording these details?

A That day, that was pretty much it. I went back to other work that I had to do.

Q When was the next time you saw this laptop?

A The next time I saw the laptop was when I removed it, and I believe it was July the 30th.

Q Okay. Now, in preparing to image this laptop, what steps did you take?

A So I went online and did some research for the model just to find some documentation about it. We also purchased a similar model at a local electronics store and began to manipulate that device to become more familiar with its form factor.

Q Showing you Government's Exhibit 7. Do you recognize that?

A Yes.

Q What is it?

A That's an email that I sent to Agent Fischlin.

MR. CHUN: Government moves to admit Exhibit 7.

MS. SCANLAN: No objection.

THE COURT: It is admitted.

(Exhibit 7 admitted.)

Q (By Mr. Chun) And what do you say in this email in the top paragraph?

A I'm telling -- do you want me to read it verbatim?

Q You can summarize.

A I'm telling Agent Fischlin that our Criminal Investigative Division in headquarters had approved a purchase of a similar laptop to the defendant's for $1,200, and that was at Fry's in Renton.

And then I'm noting that TFO Hansen, our temporary photo officer, and I spent the day, the afternoon, checking that laptop and disassembling it. We did remove the hard drive, and I also accessed the BIOS to become more familiar with that process.

We then used three different software programs, Helix, Paladin, and EnCase Portable, which we loaded onto the computer thumb drives, which we attempted to boot that test laptop from those hard drives to see if we could actually image that device that way.

Q Okay. And when did you get the test laptop?

A It was, I believe, that day, July 30th.

Q All right.

A In the morning.

Q Let's go ahead. So you get the test laptop. Run us through the steps of what you did after receiving it.

A So I initially familiarized myself with how it worked. I powered it on. Looked at its form factor, tried to identify how, if we needed to, to remove the rear panel of the device to see how easy or not it would be to access the hard drive and the battery.

Q Had you ever seen a computer with that form factor before?

A No.

Q At any point in time -- you just testified that you examined the computer to see how you would remove the back panel?

A Correct.

Q Did you ever remove that back panel?

A Of the test device?

Q Yes.

A Yes.

Q What did you learn about that test device after doing so?

A We realized that it indeed did have a solid-state hard drive, a very thin solid-state hard drive, and the battery was also fairly nonremovable.

Q In July of 2014, had you seen a solid-state drive like the one that was in that laptop before?

A No.

Q Now, what other tests did you try to run on this test machine?

A We actually did -- I actually imaged the hard drive that

came with that -- that device, to see if we could actually successfully image the hard drive. That occurred later, a few days later, using a hard-drive adapter -- solid-state, hard-drive adapter that we purchased.

Q Okay. So speaking about the test machine, did you attempt to live image it?

A Yes, we did.

Q And what test did you run?

A So those would be when I made reference to Paladin, the Helix, and EnCase Portable. Those were the -- or the softwares that we used. We had those on USB hard drives. And by accessing the BIOS and making certain commands through the BIOS, we tried to boot those operating systems from the hard drives to see if we could actually perform a live image.

Q Were you successful in doing a live image on the test machine?

A No.

Q After learning that you were not successful in doing a live image on the test machine, what was your next step?

A At that point we were -- I was pretty much resigned to the fact that we would probably have to do a traditional image of the hard drive itself by removing it.

Q Now, talking about July 30th. When you said you next saw the laptop, this is the actual defendant's laptop?

A Correct.

Q Where was that?
A That was when I physically removed it from the ECTF vault and placed it in my workstation in the lab.
Q Okay. And on that day, did you sign the log entering that vault?
A Yes.
Q And do you see that entry on Government's Exhibit 3, page 2, in front of you?
A Yes.
Q Could you just point to it?
A Yes. It's pretty much the middle entry there.
Q And on that day when you saw the laptop in the vault, did you do anything with it?
A I removed it from the vault and I brought it into my workstation and then I attached an AC-power adapter to the device.
Q Now, on July 30th, why did you plug this laptop in?
A At that point we had the -- or the test laptop, and we -- I was anticipating the possibility that we would do some type of live imaging of that device at that time, and I wanted to have it powered.
Q And just for clarification on time, when you plugged in the actual laptop, had you run your live imaging test yet on the test laptop?
A I believe I plugged it in prior to those tests.

Q And did you do any other activities with the laptop on July 30th?
A The defense laptop?
Q The defense laptop.
A No.
Q When was the next time you saw the defendant's laptop?
A It would have been on August 1st at that point.
Q And in between July 30th and August 1st, did you take any steps to further your imaging of the defendant's laptop?
A No.
Q After running the live image test on the test laptop and learning that you could not do a live image, what was your next course of action?
A At that point we -- I figured that we would need to somehow research and find an adapter for the solid-state hard drive that would enable me to plug in that hard drive into our write blocker and do a traditional image.
Q And were you able to find an adapter?
A Yes.
Q And when did you get the adapter?
A It was purchased on the 31st, and it arrived in our office on August 1st.
Q Okay. Now, on August 1st, what did you do with the defendant's laptop?
A At that point I did take the laptop, unplug the power

cord, and then I did decide that we were going to attempt to image that drive in a traditional manner.

I unscrewed the back panel and recognized and identified where the hard drive was in that laptop. At that point I began to manipulate the device in a certain way, so I could get better access to the hard drive. And I noticed that the splash screen again came up as it did on the 9th of July.

Q You say "splash screen," would that be the same splash screen that you had seen before?

A Yes.

Q Once you saw that splash screen, what did you do?

A At that point I pushed in the power button on the side of the laptop, and I turned the device off.

Q Now, before using the adapter on the actual machine, did you do any test with the test machine?

A Yes. So we used that adapter to image the test machine.

Q And how did that test go?

A It went without any trouble. In fact, I believe I did two images.

Q And so after successfully imaging the test machine, did you then move to the defendant's laptop?

A Yes.

Q Can you walk us through the steps of how you imaged the defendant's laptop?

A Sure.

So I was able to successfully remove the solid-state hard drive from the defendant's laptop. I attached it to the solid-state drive adapter and plugged it into the write blocking device, which was, in turn, plugged into my forensic computer.

At that point I launched a software program called FTK Imager. Its purpose is to use -- or it's used to image devices. I powered on the write blocker, which provides power to the solid-state hard drive and noticed that the drive was recognized by my computer. I then looked at the file structure on the FTK Imager software and recognized that it was indeed a Windows device, had the traditional Windows structure.

Q And was imaging successful?

A Yes.

Q How do you know that?

A The FTK Imager software, I generated a hash value for that image and confirmed it again as it customarily does with a recheck.

Q What is a "hash value"?

A So a hash value is a mathematical value that is generated by software, in this case FTK Imager. It's unique to a device or an image or a file. It's basically a computer digital -- digital fingerprint that identifies that image.

Q And you mentioned FTK Imager. What is that?

A That's a common computer forensic software program.
Q You say "common," does that mean it's commonly used by who?
A It's used by both law enforcement and private industry.
Q And could you actually explain what an image is?
A An image is actually an exact replica of a device or a file, in this case a hard drive.
Q You're saying the image and the original, then, are identical?
A Correct.
Q And you know that because the hash values matched?
A Correct.
Q You also mentioned, in this process, that you used a write blocker?
A Yes.
Q What is a write blocker?
A A write blocker is a small device that is typically in between the drive you are imaging and the forensic computer. It's basically a device that provides a one-way data stream, allowing the data to leave the device you're imaging and not come back to it. No data will come back on to that drive.
Q And, forensically, what is the importance of that?
A Well, it prevents any data that's from any other computer device from coming back on to that drive and potentially corrupting it.

Q And did you use one here during this imaging process?
A Yes.
Q How long did imaging this device take?
A I recall it took just over an hour.
Q And while imaging was going on, what did you do?
A I was doing other tasks there in the lab.
Q While imaging the computer, did you do anything with the shell of the computer?
A I -- at that point I did check the BIOS of the computer and -- which is the Basic Input Operating System. It pretty much just displays the date and time that's on the computer at that time, and some other functions. And I took photos of that.
Q And after imaging was complete, what did you do next?
A After the image was completed, I powered off the hard drive and detached it from the write blocker and the adapter. I placed that solid-state hard drive in a static-proof bag and then removed the battery physically from the device, placed it in a separate envelope and then taped that hard drive into the battery compartment. I then replaced the back cover of the device. And, at that point, I put it back into our ECTF vault.
Q Briefly, showing you what's been previously marked as Government's Exhibit 8. Do you recognize that?
A Yes, I do.

Q What is that?
A That is an email from myself to AUSA Wilkinson.
Q And what's the summary of what you tell AUSA Seth Wilkinson?
A I'm reiterating my notes, basically, telling him that I removed the device from our vault and took it into our lab on the 1st of August, showing the time the imaging began at 15:38 hours. And then, again, reiterated -- after removing the back cover and trying to access the hard drive, the device, quote, woke up, which is the same behavior that occurred when I removed the back cover of the test unit.
MR. CHUN: Your Honor, the United States moves to admit Exhibit 8.
MS. SCANLAN: No objection.
THE COURT: It is admitted.
(Exhibit 8 admitted.)
Q (By Mr. Chun) Showing you what's already been admitted, Government's Exhibit 10. What was this again?
A These are my personal notes.
Q And do you see an entry for August 1st on there?
A I do.
Q And do you see in your notes anywhere that you documented that the screen went on on August 1st?
A Yes. It's the second line under August 1st, "While removing the bottom panel, I noticed the device power on. I

then depressed the device's power button to power the device off. This occurred at approximately 14:45 hours."

Q And showing you what's been marked as Government's Exhibit 9. Do you recognize that?

A Yes. That's the text document generated by FTK Imager after the imaging was complete.

MR. CHUN: Move to admit Government's Exhibit 9, Your Honor.

MS. SCANLAN: No objection.

THE COURT: Admitted.

(Exhibit 9 admitted.)

Q (By Mr. Chun) And showing you what's been marked as Government's Exhibit 6. Do you recognize that?

A Yes.

Q What is that?

A That is the defendant's laptop.

Q And do you know who took these photos?

A That was myself.

Q And they're actually in the binder in front of you. There are several pages. Could you please just look through them and confirm you recognize all of them?

A Sure.

Right. They are the same.

MR. CHUN: Your Honor, the government moves to admit Exhibit 6.

MS. SCANLAN: No objection.

THE COURT: Six is admitted.

(Exhibit 6 admitted.)

Q (By Mr. Chun) Showing you page 5 of Government's Exhibit No. 6. Can you describe what that is?

A That's a photo of the solid-state drive from the defendant's laptop as it was attached to the adapter, the hard-drive adapter.

MR. CHUN: Your Honor, could I have one moment, please?

THE COURT: You may.

Q (By Mr. Chun) Showing you what's been marked as Government's Exhibit 23. Do you recognize that?

A Yes.

Q What is that?

A That's the Digital Imaging Examination Report that I generated for this case.

Q Showing you what's been marked as Government's Exhibit 24. Do you recognize that?

A Yes.

Q What is that?

A That's a supplemental report to my initial report that I submitted.

Q And showing you what's been marked as Government's Exhibit 35. Do you recognize that?

A Yes, I do.
Q And what is that?
A That is a list of some of the files that I discovered on the laptop's hard drive.
MR. CHUN: Your Honor, the United States moves to admit Government's Exhibit 23, 24, and 35.
MS. SCANLAN: No objection.
THE COURT: They're all admitted.
(Exhibits 23, 24, 35 admitted.)
MR. CHUN: No further questions.
THE COURT: Why don't we take a stretch break before you get into cross-examination.
Please be seated.
Cross-examination?

CROSS-EXAMINATION

BY MS. SCANLAN:
Q Good afternoon.
A Good morning.
Q Good morning. You're right. Good morning.
Can you either get closer to the mic or pull it closer to you?
A Sure.
Q Okay.
I want to talk first about your initial report in this case, which is Exhibit 23. When did you write that?

A That was produced in mid-August, I believe. I don't have the exact date.
Q And in that report, you indicate that your examination was pursuant to a warrant issued on August 15th, 2014, right?
A Yeah, that date is actually incorrect.
Q Another aspect of your report, which is actually Exhibit 23, page 002. Can you pull out this section right here, "Hardware use for examination." Can you see that, Agent Mills?
A Yes.
Q So, in this section of your initial report, you're talking about this is a copy also called an image. That's what you made, right, on August 1st?
A Correct.
Q It's examined with forensic software. And the software prevents adding, removing, or altering the original files, right?
A Yeah, though that should actually -- because I actually show that as hardware, the write blocker. So the correct word would be "hardware."
Q Sorry. The correct word for what?
A When it says in this -- oh, excuse me. The actual forensic software is used after the imaging, to actually look at the file structure and items that were on the disk. The actual hardware that is used is a digital write blocker,

which prevents the writing.
Q Let me summarize this for you. This sentence is about examining the image with forensic software, right?
A The last sentence there?
Q Right.
A Uh-huh.
Q And that software is designed so that it doesn't add, remove, or alter files, correct?
A Yes.
Q Why is that important?
A Well, you don't want that image to be corrupted at any point whatsoever.
Q And one way to corrupt an image is by altering the files, correct?
A That would be one way, yes.
Q Page 5 of this same exhibit. You indicate, on page 5, that best-forensic practices were used to prevent alterations to the system. Do you recall that?
A Yes.
Q So it was a best-forensic practice to leave the laptop on for 23 days in the vault?
A At that time we didn't want to touch that device any more than we had to. We didn't have a warrant yet. And so we believed it was best to leave it in its original state. As it was on, we anticipated that after we did receive a warrant

that we'd be able to image that live and capture RAM, possibly.

Q What I'm asking you, is it best forensic practice to leave a laptop you seize on for 23 days? Yes or no.

A If that's the original date and we didn't want to delete it, then, yes.

Q And by leaving it on, there are file access dates that were changed on this computer, correct?

A Yes. We saw that afterwards, yes, upon examining it.

Q And there are files that were actually modified, had different modification dates during that time period?

A Yes.

Q But you still maintain that that was the best thing to do right then?

A At what point?

Q On July 9th, to leave it on.

A That was -- according to our practice, we just -- we did not want to do that, so, yes.

Q Okay. So after you imaged the drive, you note in your report that you noticed that several files in the Windows registry had been written to, after Seleznev's apprehension on July 5th, correct?

A Yes.

Q Which registry files were written to?

A There were several registry files. From my memory, I

recall some from the system -- the system and SAM registry keys.

Q Those registry keys were written to between July 5th and July 30th?

A I believe that's somewhere.

Q So then it's not correct, then, that the last entry written to the SAM and security registry files was on July 14th, or is it correct? It is true or it's not?

A I'm not sure. You're referring to a part of my report?

Q No, I'm asking a question.

A There were some files that actually had different modified dates, yes.

Q When did you decide that you should research Windows 8.1?

A I started to research that after we received the device on July 9th.

Q You started researching it on July 9th?

A About that time, approximately. Maybe -- it may have been before that, too.

Q And so you discovered, sometime during this research around the period of July 9th, that it had Connected Standby?

A Yes.

Q July 30th, you take it out of the vault, right?

A Yes.

Q And you take it to your workstation?

A Yes.

Q And you plug it in?
A Yes.
Q And then how long is it plugged in?
A It stayed plugged in until August 1st.
Q So did it stay at your workstation until August 1st?
A Yes.
Q Is your workstation in the vault?
A No.
Q Were you with the laptop this whole time from July 30th to August 1st?
A No.
Q When you took it out on July 30th, you noticed it was off, right?
A Yes.
Q How did you notice that?
A I saw that the screen was dark.
Q But the screen was dark on July 9th when you activated the splash screen, right?
A Correct.
Q Okay. And I just want to make sure I understand.

So, on July 9th, you were looking for the serial number when you activated the splash screen?
A Yes.
Q But you know the serial number was already on the evidence log sheets, right?

A Yes.
Q So then, at some point, you start doing -- you're doing all this research, right, on Windows 8.1 and the Sony Vaio? At some point you notice that these sorts of computers may stay in what you refer to as a semi-sleep mode; yes?
A Yes.
Q And the only way to prevent this would be to remove the battery from the device?
A That's what I put in my report, yes.
Q So if you press down the power button and hold it, that's not going to turn it off?
A That would potentially turn the device off completely, yes.
Q Okay. Then I'm a little bit confused. Because if the only way to turn it off is to remove the battery, then how can you turn it off by pushing the power button?
A It is an -- an additional way of turning it off is by pushing the power button.
Q Because you actually turned it off on August 1st by pushing the power button, right?
A Yes.
Q Okay. Is there anything in your initial report about seeing the splash screen on July 9th?
A I don't believe I noted it in the report, so I might have to review it one more time.

Q Sorry. Say that again.
A I said I might have to review it one more time.
Q Okay. Do you want to review -- it's not in there. You can look at it, if you want.
A That's fine.
Q Okay. Your initial report, you indicate that Agent Fischlin received the evidence on July 9th and he inventoried it into the vault, right?
A Yes.
Q But you don't say anything at that point about you being in the vault?
A No.
Q There's nothing in the report about you being in the vault?
A No. I don't believe, no.
Q And there's nothing about leaving the laptop on, correct, in the report?
A No.
Q Nothing in the report about plugging in the computer on July 30th?
A I don't believe so, no.
Q And then on page 8 of the report, there is this section where you talk about how you couldn't figure out whether the user account, smaus, requires a password. Was that true?
A Can I see page 8?

Q Yes. It's the second paragraph. It says, "Attempts were made to find if the Windows user accounts required logon passwords. However, efforts thus far have proven unsuccessful."

A Right.

Q Do you see that?

A Yes, I do.

Q So this is a computer where you click past the splash screen and the thing comes up to enter the password, right?

A Yes, it is.

Q But you couldn't figure that out?

A I couldn't until the point that I wrote this report, no.

Q Okay. I want to switch topics and talk about the emails between yourself, Seth Wilkinson, and Ovie Carroll.

A Okay.

Q You met Mr. Carroll first on August 7 of 2014?

A Approximately, yes.

Q Is that when Mr. Carroll began working on the case?

A I'm not sure exactly when that date was. But that's the day I contacted him.

Q So at that point, in August of 2014, Mr. Carroll was working on the case, to your knowledge?

A Yes.

Q And back in August of 2014, Mr. Carroll was helping you with password cracking?

A Yes, he did.
Q In November of 2014, you sent spreadsheets with file change dates to Mr. Carroll, correct?
A Yes.
Q What file change dates?
A Those were contained on a timeline sheet that we had generated while he was there in August.
Q So did this include the 3,300 files with different access dates?
A They should. Probably did, yes.
Q And includes the two-hundred-something files with different modification dates?
A I believe so, yes.
Q But you didn't discuss either of those things in your supplemental report in January of 2015?
A No.
Q So January 5th of 2015, it sounds like the AUSAs want to know what happened on August 1st that caused the file changes; is that correct?
A Yes.
Q And it's at that point that you first tell them that it came on on August 1st?
A I don't recall if that was the first time, no.
Q Okay. So they're asking about what causes it, but they already knew?

A Well, we generated the supplemental report to explain further the behavior of Windows 8, and that was in January, yes.
Q Exhibit 10. This first entry here you have for July 9 of 2014, in Exhibit 10, it says, "The unit screen turned on and I observed" what?
A Yeah, I -- I realize that I apparently didn't finish the sentence, didn't finish my thought.
Q Do you know what you observed?
A I -- I observed the splash screen coming on, the date and time.
Q Did you go in and out of this particular vault between July 9th and July 30th?
A Yes.
Q Did you notice -- how many times, do you think?
A I couldn't remember offhand.
Q A few?
A Yeah.
Q Some?
A A half dozen, a dozen maybe.
Q At those times did you observe whether the Sony Vaio was on or off?
A No.
Q Did you look at it?
A No.

Q You decided that you wanted to conduct this Live RAM Capturer around July 30th, correct?
A We wanted to attempt an image of the device then, yes.
Q Because there is nothing in here, in your notes of July 9th or your reports, that the reason you left it on is because you wanted to do this Live RAM Capturer, right?
A No.
Q That's not in these notes for July 9th?
A No.
Q And it's not in your initial report --
A No.
Q -- right? It's not in your supplemental report?
A No.
Q Why did you think that plugging in a computer that was off would allow you to do a Live RAM Capturer?
A The reason I plugged it in to do that was to make sure that the device did have power. And I was attempting at that point in time, at any time during that day, if we were able to successfully do it with the test device, then I could immediately switch over to the defendant's device and attempt the imaging on that device.
Q But you know that you can't do a Live RAM Capturer to get the most recent powered-on data once the computer turns off, right?
A Correct.

Q Okay. So it was off on July 30th, right?
A I believe so, yes.
Q But you plugged it in to do a Live RAM Capturer that you knew wouldn't work?
A I plugged it in on the 30th with the anticipation that we'd also do an image of the hard drive while it still resided within the device.
Q But you don't need to plug in a laptop to do a regular image, right?
A Traditional image?
Q Yeah.
A No. You would remove the hard drive from the device.
Q So what does that have to do with plugging it in on July 30th?
A On July 30th, we anticipated having to have power in the device, because we'd have to plug in a USB thumb drive which contained Paladin, Helix, or EnCase Portable in this case, to boot from that hard drive. And that device would need to have power in order to enable that process.
Q So that's not the same explanation as the Live RAM Capturer explanation we've heard, right? This is a different thing?
A The two are different. The Live RAM Capturer is a separate process, and so you'd still have to have the device powered on.

Q Okay. And the test laptop that you got, right?
A Yes.
Q How similar is it to the original?
A It was very similar. It only differed in its color, and I believe the hard-drive capacity was smaller on the test laptop.
Q So is it manufactured outside the United States?
A Yes.
Q The one that you got at Fry's?
A Yes.
Q In Russia?
A No. I think it was manufactured in Japan.
Q So I want to make sure I understand. So the Sony Vaio you got here is exactly the same as the one from Russia except for the color?
A The color and the hard-drive capacity, yes, were two of the big distinctions among those.
Q Is the firmware the same?
A Did not -- did not check if the firmware was exactly the same.
Q So we don't know if that was the same. It may be something beyond the color?
A Possibly, yes.
Q How about the antennae?
A I don't recall actually inspecting the antennae on the

test device.

Q So we don't know if that's the same?

A I don't know -- I couldn't say that now, no.

Q What's the operating system in your workstation?

A My forensic workstation?

Q Yes.

A Windows 7.

MS. SCANLAN: Your Honor, may I have one moment?

THE COURT: You may.

MS. SCANLAN: Thank you.

Q (By Ms. Scanlan) I just want to make sure we're clear. The Windows 7 that was running in your workstation, was that running in August of 2014?

A Yes.

Q So you would agree at this point that it is not a best-forensic practice to have a computer with changed access dates and modification dates, correct?

A I'm sorry. Could you restate that?

Q It's not a best practice to let a computer have file changes happen to it before you image it. Is that true?

A No. I mean, the computer, if it's in a state that has sleep mode or something, it's doing what it's doing. I'm not going to interrupt that without the warrant present. I'm not going to manipulate that computer.

Q So you can't power off a device without a warrant?

A You could.

MS. SCANLAN: Okay. Thanks.

REDIRECT EXAMINATION

BY MR. CHUN:

Q Is your workstation secure?

A Yes.

Q Can you describe where it is and the security around it?

A It's located in a lab. It has the same or similar security features as our FTK vault. And it has an electronic keypad, as well as an additional cyberlock.

Q And earlier you were asked about not being able to identify whether a login password was necessary. You wrote that in your report.

When you were examining this computer at that time, how are you -- are you actually on it like a user who would log in and see a Windows' screen and type in a password --

A No.

Q -- or are you looking at it in some other way?

A No. I'm just looking at it, in this case, in a media, in the forensic software that I was using.

Q And that's very different from how a user --

MS. SCANLAN: Objection; leading.

THE COURT: It is leading.

Q (By Mr. Chun) How is that different from how a normal user would interact with the computer?

A A normal user would interact in the way that we're familiar with by typing and swiping. In this case, it had a touchscreen. I reviewed the data of that image in a computer forensics software. In this case, it's called EnCase, which shows the details of every single file that's located on a computer.

Q What was the purpose of buying a test machine versus running actual tests on the laptop?

A I wanted to be very familiar with the form factor of that laptop. I didn't want to touch the defendant's laptop until I felt comfortable myself with how to approach the imaging of the system.

Q Is that a precautionary step?

A Yes.

MR. CHUN: No further questions, Your Honor.

THE COURT: Any further cross?

MS. SCANLAN: No, Your Honor.

THE COURT: Any objection to this witness being excused by the government?

MR. CHUN: No objection.

MS. SCANLAN: No objection, Your Honor.

THE COURT: You may step down.

Counsel, your next witness.

MR. CHUN: The United States calls Ovie Carroll.

MR. BARBOSA: Your Honor, may this witness remain in

the courtroom?

THE COURT: If he's not going to be recalled to testify.

OVIE CARROLL, HAVING BEEN FIRST DULY SWORN, TESTIFIED AS FOLLOWS:

THE CLERK: Please state your first and last names, and spell both for the record.

THE WITNESS: It's Ovie Carroll, O-v-i-e, C-a-r-r-o-l-l.

THE COURT: You may inquire.

DIRECT EXAMINATION

BY MR. CHUN:

Q How are you employed?

A I'm currently employed as a Senior Executive for the Department of Justice, and the Director of the Cyber Crime Lab.

Q How long have you been with the Department of Justice?

A Ten years and six months.

Q And how long have you been the Director of the Cyber Crime Lab?

A Ten years and six months.

Q And what are your duties as the Director of the Cyber Crime Lab?

A As the Director of the Cyber Crime Lab, I run the Department of Justice's Cyber Crime Lab. And we support

prosecutors across the country in any high-tech crime case, where the capabilities or efforts of the investigative agencies is in line with the needs of the prosecutor.

I also am the Senior Executive, what they consider the Senior Advisor to senior DOJ officials on high-technology crime matters. So regardless of the type of the case, if the attorney general or the deputy attorney general has a case that involves high technology that they need to understand the technology or know something about it, I'm the primary one they come to.

Q What did you do before joining the Department of Justice?

A I was a Special Agent in Charge of the Technical Crimes Unit for the Postal Inspector General's Office.

Q And what were your duties there?

A Well, I was in charge of the three units, the computer forensics section, the computer intrusion section, and the technical services section.

So the computer forensics obviously does digital evidence. The computer intrusion does investigating of intrusion, compromises, hacking cases. And the technical services are the ones that do all the high-technology wires, bugs, surveillance cameras, that type of thing.

Q And how long were you there for?

A I was there for five years.

Q And what did you do before joining there?

A I was the Special Agent in Charge of the Washington Field Office Computer Investigations Operations Branch. That was for the Air Force, Office of Special Investigations.

And there, we were in charge of all intrusions into Department of Defense systems that had any impact or effect on the Air Force, as well as forensics for any significant cases across the country.

Q How long were you there for?

A There, I was -- well, with the OSI and the Air Force, it was 15 years. So this is my 30th year in law enforcement.

Q So, approximately, how many years had you been involved in computer and digital forensics?

A About 20 years.

Q And in becoming a forensic examiner, what type of training have you received over the years?

A Well, my official training, probably like a lot of forensic examiners, I started learning on my own before it became a profession.

And then when the Air Force Office of Special Investigation started up their computer forensics program where they decided they needed agents who understand and knew how to do digital evidence, they had invited me to be one of the pilot or the first people to go through this training and be, what they called at the time, a computer forensics field examiner.

Q Have you received other training over the years in improving your forensic examination skills?

A We do routine training. I've been through pretty much all the training for the Air Force. The Department of Defense has training in Glynco, Maryland.

And I go through annual training, also, in private vendors, whether it be the SANS Institute, AccessData. Any software companies that's teaching computer forensics, we try to experience that training and benefit from it. So we have -- the computer forensics moves so fast that you have to constantly be in training to keep up with it.

Q Now, do you teach or conduct training courses at all?

A I do. I actually have two part-time jobs. One, I'm an adjunct professor for the last eight years with George Washington University, where I teach cyber investigations for their master's degree program.

And I'm also a certified instructor, as well as a coauthor for the SANS Institute, the Advanced Windows Digital Forensics course.

Q What is SANS Institute?

A SANS Institute is an international training company. It started off with just security, audit, and networking type of training first for administrators. And it has grown over the years to include things like white-hat hacking, reverse engineering, computer forensics, computer intrusion

investigation. So now they pretty much teach -- almost anything that has to do with computers, they have a course for it that I teach internationally.

Q You say international, do you teach internationally?

A I teach internationally for both the SANS Institute, as well as for the Department of Justice.

Q And so who are you teaching or training?

A With the SANS Institute, it's pretty much anybody, anybody that can afford to go through the training classes. They're relatively expensive. But anybody who can afford to go to the training classes.

I've had defense attorneys. I've had government employees, NSA, CIA, law enforcement, defense attorneys. I even had one state or local judge wanted to go through one of the classes. So, really, just anybody. We've even had some prosecutors go through the class.

Q And do you teach domestically also?

A Yes, extensively.

Q For SANS or DOJ?

A Both.

Q And who are you training domestically?

A In my DOJ capacity, my primary customer is the prosecutor. So I do -- most of my training is with Department of Justice prosecutors. I do training to others, but it all comes secondary to training prosecutors.

Q Are you a member of any forensic-oriented professional organizations?

A I am. I am the task group chair for digital evidence on the Organization for Scientific Area Committee. It is an international body for digital evidence. I'm a member of the Scientific Working Group on Digital Evidence. I am also on the Federal Advisory Board for AccessData, the company that makes FTK.

And I'm also a consultant, an unpaid consultant, for several of the forensics tools. So like with AccessData, the people that make FTK, I'm routinely called and brought in by the CEO for AccessData and the COO, to give them advice on their tool, what changes need to be made, any issues with the tool, et cetera. And I do that for many different vendors.

The primary ones that use me the most is AccessData, something called Magnum Forensics that makes Evidence Finder, and a couple of other tools, and Nuix, which is another forensic/e-discovery tool predominantly for email. Well, I believe it's mainly for email.

Q In your career as a forensic examiner, how many computers have you reviewed, approximately?

A Hundreds or thousands. I couldn't -- I'm sorry, I couldn't possibly put a number on it, but I know it's hundreds or thousands in 20 years.

Q Of those, how many run a variation of Windows?

A You know, a large majority of everything that we see for forensics is Windows. And that makes sense, because Windows has probably 90 percent of the market share, 89 percent. So I'd say, 80, 90, even higher, have to do with Windows computer systems.

We are starting to see more Mac Forensics or Mac computers. They are getting more popular. And when we work intrusion cases, patent cases, it's common to see Linux computers. But, again, I would say the Mac and the Linux, probably ten percent of what we do.

Q As part of your teaching, is Windows 8, specifically Windows 8 and 8.1, part of what you teach?

A Oh, absolutely. In the SANS course, we teach forensics on everything we -- we start with Windows XP, even though it's no longer supported. We teach the forensic artifacts in Windows XP, what's different in Vista, what's different in 8, 8.1. We teach all the variations of Windows starting with Windows XP up through Windows 10.

MR. CHUN: Your Honor, unless there is an objection, I anticipate asking or eliciting opinion testimony from this witness.

THE COURT: Any objection?

MS. SCANLAN: No, Your Honor.

THE COURT: The witness may proceed as an expert. Counsel, we'll take our noon recess at this time.

(COURT IN RECESS.)

THE COURT: Counsel.

MR. BROWNE: First of all, the gentleman from the U.S. Attorney's Office just informed us that there is indeed a SIM card in this computer that they just discovered over the noon hour.

THE COURT: In which computer?

MR. BROWNE: Mr. Seleznev's computer, Exhibit 1. So which means, obviously, what we've heard so far, it's capable of connecting to the Internet which kind of changes everything that we've been doing theoretically.

The first thing I want to let you know is that the gentleman told us that, and I appreciate that. And I really appreciate Agent Mills checking on that and telling us that.

And the second thing I want to bring up is, we did not think there was a motion to exclude witnesses. So we've had our witnesses here listening to expert testimony with the suspicion we may call them back.

You said something before the noon hour that led me to believe that maybe that's not true.

THE COURT: Counsel, the normal practice the court has is, after the witness concludes their testimony, I always inquire of each of the lawyers if there's any objection to the witness being excused. That's intended to elicit the desire and concern about bringing that witness back and let

the court know at that point in time.

Otherwise, once that witness completes the testimony, they're free to remain in the courtroom. That's been this court's practice in this court, the court practice in the Superior Court for 13-and-a-half years.

MR. BROWNE: So he can testify again?

THE COURT: No. Once they're excused, that's it. All right. You may continue your examination.

MR. CHUN: Thank you, Your Honor.

Q (By Mr. Chun) Mr. Carroll, are you familiar with the case here, United States v. Roman Seleznev?

A I am.

Q When were you first asked to consult on this case?

A Consult on the case would have been probably August of 2014.

Q And what were you asked to do at that time?

A At that time, it was the United States Attorney for the Western District of Washington. She had called me personally and asked if I would mind coming and being a consultant to the forensic examiner for the Secret Service.

Q So, I guess, you say "consultant." What does that mean versus being an actual examiner?

A What I do, a large part of my job is, I come and I provide technical advice and consultation to the people that are actually doing the analysis. Some of that feels like

training. So I'll say: Hey, have you looked at this forensic artifact? Do you know about this? This particular artifact had this information. So what is it that you're looking for, and I can advise on which artifacts will be best to identify the information that you're looking for.

Q And, at some point in time in this case, were you asked to review the defense expert reports?

A I was.

Q And were you asked to prepare a report in response to the defense experts' findings as well?

A I was.

Q And in doing so, what did you examine?

A I examined the forensic-image file of what was told to me to be Roman Seleznev's Sony Vaio laptop.

Q And did you get the whole laptop and hard drive, or just an image file?

A No, just the forensic-image file.

Q And did you produce a report?

A I did.

Q Showing you what's been marked as Government's Exhibit 27. It's also in the binder up there in front of you. Do you recognize you?

A I do. This is the report that I produced.

Q I'm showing you the first and last page.

MR. CHUN: Government moves to admit Government's

Exhibit 27.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 27 admitted.)

Q (By Mr. Chun) Now, in testing the image of Mr. Seleznev's laptop -- I'll withdraw that.

Yesterday, you heard Mr. Blank testify that there is a possibility that this computer after it's seized by the law enforcement, that someone remotely logged on to this computer.

Do you agree with that?

A No, not at all.

Q Why not?

A Well, my examination of the computer showed it had not connected to any network subsequent to the 5th of July. And it would be impossible to connect remotely to a computer that doesn't have network access.

Q And did you examine the laptop to see what the last network it connected to was?

A I did. The last network it connected to was the Kanifushi network, which I understand to be the wireless network at the hotel.

Q Showing you Government's Exhibit 16. Do you recognize that?

A I do.

Q What is it?
A That's a screenshot that I made of the network list of profile's registry key.
Q And so is this something you created?
A It is. It is a screenshot that I created.
MR. CHUN: Government moves to admit Exhibit 16, Your Honor.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 16 admitted.)
Q (By Mr. Chun) Could you please describe what we see here?
A Well, this is one of the registry keys. Windows, one of the functions it does is, it creates a log or it remembers every network that this computer connects to, whether it's wired or wireless or what have you. And this is one of the registry keys, the network profile key. It documents every network you connected to, the first time you connected to that network, and the last time you ever connected to that network, as well as how you connected to that network.
There are other registry keys that are duplicative of this that have other information, like the serial number or the Mac address of each network that you connected to. But this is, typically, the network keys that I look at for networks, because it lists them all. And I can tell the first time and last time they ever connected.

Q Do you know what the last network it connected to was, updated by this key?

A Yes. As you can see by the profile name at the very top, that's the Kanifushi network. So that was the name. The very top on the right is the name of the network that it connected to.

Q And I see on this exhibit, this box here I've highlighted. It says "Decode on top." What is that?

A That's just another program that we use in forensics. A lot of the date/timestamps inside Windows and other applications, they're not regular date/timestamps. They're encoded.

So if you zoom back out of that for a moment. Let me show you something. If you could zoom into this area here. So you see those? You see where it says "Date created" along the left-hand side here? You have one called "Date created," and the last line is "Date connected."

Here is "Date connected," and there is "Date created." So the date created, you see this number right here? This is what they call 128-bit system timestamp. So that's actually a date, time, and second, and millisecond of the first time that this computer ever connected to that particular network.

And then below that, the last line where you see date last connected, that is another 128-bit system timestamp. That is the last time this computer connected to that wireless

network.

Q So based on that, what date and time did this first connect to Kanifushi?

A This first connected to the Kanifushi network, it registered at 21 June, at 20:47:55, and that's local time. And the last connected, the box highlighting here, is when it last connected to the Kanifushi network on July 3rd, at 21:55:18.

Q Does this key tell you how this computer connected to the network?

A Yes. If you zoom in this area right there, do you see this line right here, "Name type"? Right here that I'm drawing, that "Name type." And if you come over here, that number right there, that 47 that I just circled, that 47 indicates they connected to it through wireless, 802.11.

If, instead, they would have plugged in a regular network cable, a regular Cat-5 network cable, that number would be 06. So this tells us the first time/last time, and how they connected to that network.

Q And I'll show you Government's Exhibit 14. Do you recognize this?

A I do.

Q What is it?

A It's another screenshot that I created of the Windows network profile/operational event log.

MR. CHUN: Your Honor, move to admit Government's Exhibit 14.

MS. SCANLAN: No objection.

THE COURT: Admitted.

(Exhibit 14 admitted.)

Q (By Mr. Chun) So what is the network profile/operational event log?

A This is an event log Windows keeps to also track when computers connect to and disconnect from networks.

Q And what information do you see here? We'll start with the top box, the box in red.

A The top box is actually the last entry in this log. So what this is showing us here, in this last entry, is that at 5:37, on the 5th of July, was the last time this computer recorded that there was a network connection. And it's here showing that the state of that network connection is disconnected. See down here? Right there, it says the state is disconnected. So that's showing it disconnected from the Kanifushi network. Recorded disconnected.

Q Showing you Government's Exhibit 15. Do you recognize that?

A I do.

Q What is it?

A It's another screenshot of an event log I created.

MR. CHUN: United States moves to admit Government's

Exhibit 15.

MS. SCANLAN: No objection.

THE COURT: Admitted.

(Exhibit 15 admitted.)

Q (By Mr. Chun) Describe what this is.

A This is just another event log showing when networks are connected to and disconnected. This one seems redundant to the one that you just showed me. But this one specifically is Wireless LAN. So you see right here, the network log is Wireless LAN. And this one is showing the last event log in this was on the 7/5, July 5th, at 5:37.

And down here, you see this says, "This Wireless LAN auto-config service has successfully disconnected from the wireless network." I know it seems redundant to the last one we looked at, but this one is specifically wireless.

Q Showing you Government's Exhibit 22. Do you recognize this?

A This looks like the Windows update log. This is the screenshot of the -- yep, this is the screenshot of the Windows update log that I created.

MR. CHUN: United States moves to admit Exhibit 22.

MS. SCANLAN: May I inquire?

THE COURT: You may.

VOIR DIRE EXAMINATION

BY MS. SCANLAN:

Q Mr. Carroll, the red box that says "source."
A Yes, ma'am.
Q Did you add that box?
A I did. I added that box, as well as this red box showing you, right here, where that log came from on the computer.
Q So just so I understand, when looking at these exhibits, the stuff in red on these exhibits is yours?
A Yes.
Q Is that right?
A Yes.

MS. SCANLAN: I have no objection.

THE COURT: Just for clarification, counsel referred to "the stuff in red." Anyplace that's highlighted in red on 22, 15, or 14, that's in red, same answer?

THE WITNESS: Yes, sir.

THE COURT: Okay. With that understanding, 22 is admitted. You may proceed.

(Exhibit 22 admitted.)

A I do that, because if I just give them a log, they don't know why I'm showing it to them. So I typically want to bring their eyes to, this is the log I want to explain.
Q (By Mr. Chun) What is the Windows update log?
A It's just a log file, like an audit log file. Windows is routinely trying to connect to the Internet; and so, phone home to Microsoft, to see if there are any updates to your

operating system.

So this is one of the logs that's kept to show that it is trying to connect to Microsoft and see if there is any updates to download.

Q Showing you page 2. There is a red box which you added, correct?

A I did.

Q And what was the purpose of that?

A Well, the reason why I highlighted this box is, you can see, right here, that this shows every time that Windows in this particular log tries to connect to the Microsoft server, it tells you what's its status. And, in this case, this is the last time in this log that it shows that the network state is connected.

So this is showing at 5:09, on the 5th of July, it was connected to a network. And so when it tried to check with Microsoft at 5:09, it actually had a network connection and it recorded that in the log as network state/connected.

Q Going to the next page 3 of the same exhibit. What do you see on this page?

A I highlighted several subsequent pages like this. And this is just showing you that also on 7/5, later in the day at 22:37, the network state showed as disconnected. And throughout the rest of this log till the very end, all subsequent network states are disconnected.

Again, this is just corroborating the fact that this computer no longer had a network.

Q And going to the last page, page 17. What do you see here?

A It is just the last page of the audit log. Again, showing you that all the way through after 7/5, it never regained a network connection.

Q So your testimony is, you reviewed the logs all the way through up to page 17, which you're saying is the last one?

A Yes.

Q Did you find any other connection after that last connection?

A No. The last network connection that it recorded in this log was on July 5th, the first page that you showed.

Q Showing you what's been marked as Government's Exhibit 47. Do you recognize this?

A I do.

Q And this is a two-page exhibit. What is it?

A This is the output of the -- Microsoft Windows, starting with Windows 8, created this database that is keeping track of information about your computer for diagnostic purposes. Generally speaking, the users don't use this.

Q So did you create this exhibit?

A I did. I created this exhibit.

MR. CHUN: United States moves to admit Government's

Exhibit 47.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 47 admitted.)

Q (By Mr. Chun) Please describe what we're seeing here.

A So the diagnostics log is called -- we call it SRUM. It stands for System Resource Usage Monitor. And this log is keeping track of all the applications that are running, all the networks that it's connected to, the bandwidth that's going in and out.

This is really, in the forensics' community, an exciting artifact. Because if a company gets hacked or something happens, you can see every application, how much bandwidth was coming into your computer and how much bandwidth was going out of your computer.

Q I'm going to highlight a top portion here. Could you please describe what we're seeing in regards to the columns?

A Sure.

So this column right here called "App ID," this is just saying this is the application that was running. The next column is titled "User ID," and that's the user's security identifier. So this is how the computer identifies who is responsible for running that particular program or application.

If you move further, this is the interface, and it tells,

okay, what network? How did it connect?

And as I mentioned, the Kanifushi network they connected over wireless, and so the technology that it used was 802.11. You can see 802.11 right here.

And then this box is what network did you connect to. It's the Kanifushi network.

And, lastly, we have how many bytes were into this computer and out of this computer for each of these applications at that time.

Q And looking at this exhibit as a whole, could you tell us what the last network this computer connected to was?

A Yes. This last network, you can see right here, is Kanifushi network.

Q The second page of this exhibit, can you describe what this is?

A This, I believe, is the last page -- these are the last entries of this log. And so you can see the last network that they connected to was the Kanifushi network right here. And this is keeping track of how long the network had been connected.

Q And so would this be -- I noticed the top title here that you've entitled as being the "SRUM network connectivity"?

A Yes.

Q And then the first page, you had called it the "Network data usage"?

A Uh-huh.
Q Are those different logs?
A They're two different tables out of the same database. So one database tracks the applications that are using the Internet or the network.
The other log tracks to the -- if you switch to the next page. The other network tracks the network itself, which network it's connected to.
Q Okay. And what would be your conclusion as the last network this computer connected to?
A Well, as this log clearly shows, the last network it connected to was the Kanifushi network here.
Q And what would be the date and time there?
A 7/5. July 5th, 17:38.
Q Now, yesterday you heard from defense experts that this computer could have connected to unknown wireless networks or Wi-Fi networks while in Connected Standby. Do you believe that happened to this computer?
A No, absolutely not. In fact, if it would have connected to networks, there's several forensic artifacts like we just talked about, the SRUM database would have recorded the network it connected to, the event log would have recorded it, several registry keys would have recorded it. So I'm sure that it did not connect to another network.
Q And yesterday you heard Mr. Blank testify that covering up

a remote logging connection by Wi-Fi is something that you'd learn in basic hacker school, I believe is the phrase he used.

Do you agree with that?

A No.

Q Why not?

A Well, quite honestly, I've seen some basic hacker schools. And doing this for 20 years, I don't know of any hacker that knows all the forensic artifacts that combine the expertise of Mr. Lahman and Blank and myself and Mr. Fischlin and Mills. So, no.

In hacker school, they do try to teach you things to get rid of. But they just don't know all the forensic artifacts that we do in the forensics' community.

Q Also yesterday, you heard Mr. Lahman's testimony that someone logged on to the computer on July 7th, 2014. Do you agree with this opinion?

A No.

Q Did you examine this laptop to see who the last user of the login was?

A I did.

Q And what did you find?

A The last user account to log in was the user account named smaus.

Q And showing you what's been marked as Government's Exhibit

17. Do you recognize this?

A Yes. This is the security event log that I had took a screenshot of.

MR. CHUN: Your Honor, the United States moves to admit Government's Exhibit 17.

MS. SCANLAN: No objection.

MR. CHUN: And just for clarification, Your Honor, this was conditionally admitted yesterday as a one-page exhibit. The United States, over the evening, has added a second page and provided it to counsel. So if there was a change, it will be in 17.

THE COURT: Any objection?

MS. SCANLAN: Sorry, Your Honor. I didn't hear. I have no objection, and I'm aware of both pages.

THE COURT: All right. Previously, the court admitted on a condition. My question, do you have any reason for the court to keep the conditional admit intact?

MS. SCANLAN: No. I think this is the proper witness to introduce that exhibit.

THE COURT: Exhibit 17 is fully admitted. Conditional limitations are removed.

MR. CHUN: Thank you, Your Honor.

(Exhibit 17 admitted.)

Q (By Mr. Chun) Mr. Carroll, could you please describe what we see here in Exhibit 17?

A Yes. I drew this red box around the last logoff for a user in this log. So this shows you an event ID 4647, that the last user logged off on 7/5 at 2:24:49. So that's when that was recorded.

Q And what is the purpose of the security event log?

A Well, the security event log is the authoritative, most reliable means of documenting logons and logoffs onto a computer system.

Q So if you're wondering who logged on to a computer, are you saying this is the primary artifact to turn to?

A It is. And this is always the first artifact that you turn to.

Q I'm looking at this red box that you testified about being July 5th, 2014, at 2:24:49 a.m. Above it, a later date and time, there are other entries showing logon and logoff?

A Yes.

Q What are those?

A Any application or anything that runs on a Windows computer has to have permissions, and so that includes system permissions.

So all these subsequent logons/logoffs are the system, such as the Windows system has to run so it will actually show a logon. And that's what you're seeing here with different logons and logoffs.

If you go down to the bottom that shows what is inside

that log that I highlighted, if you look at the bottom of this, this is the contents of the box that I had highlighted showing the last user was smaus, and this is his security identifier.

Remember, I told you that the computer remembers people by their security identifier, not necessarily their name. And as you see here in the event log, it shows this event generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.

So this shows that the user account, smaus, logged off.

MR. CHUN: Your Honor, this exhibit is now three pages, not two pages.

THE COURT: Does counsel have a copy of page 3?

MS. SCANLAN: I do.

THE COURT: Any objection to -- let me ask you first, counsel. Are there any more pages to Exhibit 17?

MR. CHUN: I apologize, Your Honor. There are not.

THE COURT: Counsel, any objection to admission of Exhibit 17 in all three pages?

MS. SCANLAN: No.

THE COURT: 17, in its entirety, is admitted.

(Exhibit 17 admitted.)

Q (By Mr. Chun) Looking at page 2 of this exhibit, can you tell us what this is?

A You had talked about subsequent logons and logoffs. So this is just an example I thought I would show of another logon after the user smaus logged off. And, in this case, you can see the user security identifier as S1518, and the account name is DWM, desktop/Windows manager. So this is one of those system events.

Q And now showing you page 3 of this exhibit. Could you please explain what this is?

A This is the last event log in this event. This is the last entry in this event log. And this is just, again, showing another system here, the same S1518 logging a special logon.

Q As part of your examination, did you examine every logon/logoff after June 5th, at 2:24:49?

A I did.

Q Were there any other user logoffs?

A No, there weren't.

Q Showing you Government's Exhibit 41. Do you recognize this?

A This is just another event log that I highlighted -- oh. This is an event log showing the last logon right here. You can see it's an account that successfully logged on.

And this was the last time that the user smaus -- or, right here, the "romarigoro," the user account for smaus, logged on to this computer. So this is just recording the

last time the smaus user account logged on.
Q So comparing what we saw before logoffs, this would be a logon, right?
A Uh-huh.
THE COURT: Was that a yes?
THE WITNESS: Yes.
MR. CHUN: Move to admit 41.
MS. SCANLAN: No objection.
THE COURT: Admitted.
(Exhibit 41 admitted.)
Q (By Mr. Chun) Showing you Government's Exhibit 19. Do you recognize this?
A I do. This is a screenshot that I took of what's called a SAM registry hive.
Q And just to show you Exhibit 20, do you recognize this as well?
A Yes. This is a screenshot of the software registry hive.
Q And these are both screenshots you took?
A I did.
MR. CHUN: United States moves to admit 19 and 20.
MS. SCANLAN: No objection.
THE COURT: Admitted.
(Exhibit 19 and 20 admitted.)
Q (By Mr. Chun) Going back to Exhibit 19, could you please explain what we see here?

A Are you familiar with what a registry is? Should I leave that alone? Should I --

Q Explain what a registry is.

A So what makes the Windows computer system run is these registry hives. And registries are kind of like databases, and there are two types of registries. There are core registry hives. Those are for the Windows system. And then there are user registry hives.

In the core registry hives, one of the core registry hives is something called a SAM registry hive. And in that, it keeps track of all the user accounts that have accounts on this system. So any time that they're logging in, they have a user account on the system. This particular screenshot shows this is the security identifier. As you can see, it's 1001. This is just the short version of the smaus user account's security identifier.

As I said, Windows commonly recognizes and refers to the users not by the name of smaus, but rather by their secured identifier. And in the SAM registry hive, it just shows you the last four of the security identifiers.

So I took a screenshot showing that the user account smaus -- the box that is highlighted that I put there, the red box, it shows that user account smaus had a security identifier of 1001, the last characters.

And that also belonged -- if you look in the bottom

right-hand corner, that also is associated to the romariogro.mail.ru email address.

Q And showing you what's been marked Exhibit 20 here. Could you please describe what we're seeing here?

A Uh-huh. This is the software registry hive. And the reason why I took this screenshot is, in the previous screenshot of the SAM registry hive, remember it only showed you the last four.

If you can zoom in right here for a moment. In the last screenshot, you noticed that it only showed you the last four, which is the 1001. So what I wanted to do was show the prosecutor the full security identifier, which is what we see in a lot of the other logs, event logs, SRUM, et cetera.

Q And what would this top red box tell you?

A And this was just further trying to explain that that security identifier belongs to the user smaus, and his home directory is located under C: user smaus.

Q And these are the identifiers that you see under other logs and keys that identify this user?

A Yes.

Q Showing you what's been marked as Government's Exhibit 18. Do you recognize this?

A Yes. This is a screenshot that I took of the output of the application resource table in the SRUM database. Remember that database that keeps track of system diagnostic

information and events, this is one of those tables. This particular table is keeping track of every application that's running and who is responsible for running that application.

So I drew a red box here to show you that the last applications that were run by the user with any user account, and this is the smaus user account, was Firefox and Tor. So, see right here? There is -- Firefox and Tor were the last two applications. And they were run with the user ID of smaus, the 1001 security identifier.

MR. CHUN: United States moves to admit Exhibit 18.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 18 admitted.)

Q (By Mr. Chun) At what time and date were those run?

A Those were recorded in the SRUM database at 2:24, on July 5th.

Q And are those recorded realtime?

A No. The SRUM database is not recorded realtime. The SRUM database records data on the hour or every hour, or it tries to record every hour.

Q Showing you what's been marked as Government's Exhibit 21. Do you recognize this?

A Yes. This is the output of the USN journal log.

MR. CHUN: United States moves to admit 21.

MS. SCANLAN: No objection.

THE COURT: Admitted.

(Exhibit 21 admitted.)

Q (By Mr. Chun) Could you please describe what we see here?

A The USN journal log is essentially like a flight record, the black box on an aircraft. And it's trying to document the files that are touched so that applications, as they're working, can know what's changing as I'm operating. So I know what's old, what's new. What do I need to update? And this is just -- I kind of refer to it as a little bit of an audit log.

Q And did you review this USN journal for activity attributable to a user?

A I did.

Q And what did you find?

A Well, if you notice here, we've got this particular file or this particular column represents the full filepath of the files that were accessed and recorded in the user journal log.

And so what I did is, I reviewed all of these files in the user journal log, looked at where they were located, and what they do essentially, to determine that none of these were user files. These are essentially system actions. You can see the system working.

Q And this is a multipage exhibit. Going to the last page here.

A Oh, yes.
Q Could you say what the last page is?
A 669.
Q So this is a long journal?
A Yes, this is a long journal.
Q So you're saying -- did you review for all activity after July 5th?
A I did.
Q And did you find any -- what was your findings of activities after July 5th?
A My findings were that none of the files were a result of user activity.
Q Showing you Government's Exhibit 48. Do you recognize this?
A Huh.
Yes. This is a screenshot that I took of the software registry key. And it is the Winlogon registry key that the other experts had testified to.
MR. CHUN: The United States moves to admit Exhibit 48.
MS. SCANLAN: No objection.
THE COURT: Admitted.
(Exhibit 48 admitted.)
MR. CHUN: Your Honor, may I have one moment?
THE COURT: You may.

THE WITNESS: May I explain?

Q (By Mr. Chun) Could you go ahead and describe what we see here?

A What you're looking at here is not -- what you're looking at here is the results of a test, of a series of tests that we conducted in our lab; whereby, I restored the forensic image to a hard drive, much like the defense did. And I placed this into a computer, turned the computer on, then shut the computer, removed the hard drive, and examined the Winlogon registry key.

And what you'll notice down here at the bottom, the last write time -- if you could zoom into that. The last write time was 5/24/2016, at 14:29. And that was when I put that restored image of the computer into a laptop and turned it on. Now, I did not log in. It just went to the splash screen, yet it updated this Winlogon key.

Q Let's take that step by step. Yesterday you heard testimony from the defense experts that somebody logged on to this computer, and that conclusion was based on a Winlogon registry key?

A Right.

Q What is the Winlogon registry key?

A Essentially, the Winlogon registry key tells the variables. It has -- in this particular case, with this particular computer, it had 24 different variables that it

would feed to the computer when it boots up, when users log in at different times.

And so it's -- it tells it what shell to use, different types of variables that the computer would want to know about the environment when you start the computer or log in.

Q Showing you what's been marked as Government's Exhibit 42. Do you recognize this?

A Yes. This is a screenshot they took of the Winlogin key as it was on Mr. Seleznev's computer, the Sony Vaio, when we looked at the forensic image. As a matter of fact, this is the same registry key that the defense experts presented with the last logon date of 7/7, at 19:46.

Q And showing you what's been marked as -- you heard yesterday, Mr. Lahman testify that the date change in a Winlogon key is the definitive proof of someone logging on. Do you agree with that?

A No. It's not true.

Q Why not?

A Why isn't it? It's just not true.

The Winlogon key gets updated at other times. It is not reflective of the last time someone logged on. We conducted several tests in the lab. I think I conducted five or six tests where we restored the image, put it into the computer at different times. And every time we start the computer with that restore image, it updates this key and shows you

the date that you started that computer, even though you never logged in.

Other times, we shut the computer down, restarted it, and let the computer sit. At one point, we let it sit for an hour. At another point, we let it sit for two hours. At one point, we let it sit for 24 and 48 hours.

And, in one instance, after 24 hours, even though it's not logged in -- we never logged into it. It was just at that splash screen -- the Winlogin key updates.

So, again, this is not a forensic artifact that I know of in the last twenty years that anybody has used to suggest that this documents every time someone logs in. This is just a misinterpretation of what the Winlogin key does.

Q Going back to what you just said about your experience with the Winlogon key. Have you ever heard anyone refer to it as definitive proof that someone logged in to it?

A No. As I've said, I've been doing forensics for 20 years. The fact that I'm at the Department of Justice, I have this advantageous role where I can key over forensic exams done across the country. And I've never even heard of any other forensic examiner presenting this key as definitive proof of when people logged in to the computer.

Q And just to clarify your earlier testimony. Was it that you tested this theory, and you found that this key would change even without logging on to the computer?

A Yes. We tested this multiple times in the lab, and the Winlogin key would update.

Q Going back to 48, previously admitted. Could you describe this briefly?

A This was one of the tests that we connected on 5/24, May 24 of this year, at 14:29. And when we booted the computer, then closed the lid, removed the hard drive, examined the Win registry key, this is what we saw; that it was updated just by booting the computer up and getting the splash screen and going no further.

Q Now, showing you what's been marked as Government's Exhibit 49. Do you recognize this?

A This is one of the screenshots that I took of the output of the USN journal log.

MR. CHUN: Move to admit 49, Your Honor.

MS. SCANLAN: No objection.

THE COURT: Admitted.

(Exhibit 49 admitted.)

Q (By Mr. Chun) Can you describe what this shows?

A Well, in response to some of the defense testimony where they said all these files have access times after seizure of law enforcement, I wanted to see if we could determine what might cause that.

And, in looking at this log, you can see that 60 seconds before all those link files had their last access time

updated, you see here in red the McAfee antivirus log files being updated. And approximately 120 seconds after all those linked file access times were updated, you again see, in kind of an orange and brown, again McAfee antivirus active and writing to log again.

So this is just consistent with why those access times may have been updated.

Q All right. And, I guess, moving back to the issue of someone logging on to this computer. Yesterday you heard testimony that covering up a login is also, I believe, something you learn in basic hacker school.

Would you agree with that?

A To an extent. Most of the ways -- most of the ways hackers will try to cover up somebody logged in is they'll clear the event logs. There will be no event log. They clear them all.

Q And what about an instance here where there are logs?

A Well, it would -- as I think the defense's expert had previously testified, you'd have to -- you'd have to go through extraordinary measures to try to individually edit out a single event log. And that would be highly unlikely, because each event log in each one of the logs have their own record number. So they're sequence. So every log that gets written in an event log, gets a sequence number.

So if you deleted the fact that I logged in or someone

logged in to the computer system, not only would you have to delete that event log, but you would then have to renumber all the subsequent event logs so that it matched. And you'd have to delete all the other forensic artifacts that may possibly show that a user logged in.

Q So is it your opinion that this would be a difficult task?

A I think near impossible to pull off successfully.

Q Now, you also heard that there are 274 files that had been modified after July 5th, 2014. Did you examine the computer for files that had modification dates after July 5th, 2014?

A I did.

Q And how many files did you count with that date?

A I counted roughly the same number of files that the defense did, around 273, 274, if you include blank directories and things. Actual files themselves, I think it was more like 188. But I'm not arguing with the 273 or 4.

Q Did you review each of those files?

A I did.

Q And what was your conclusion after reviewing them?

A Well, again, they were very consistent with all of our other findings and all the other evidence on the computer, which they were a result of things like the Sony Vaio Home Improvement Program active on the computer, the antivirus program running, prefetch files, normal system maintenance and operation.

Q And Mr. Blank --
A No more user-initiated files.
Q Mr. Blank also testified that he observed about 3300 files of last access dates after July 5th of 2014. Did you also review those files?
A I did.
Q Did you find about the same number as well?
A I did.
Q What does "last access" mean?
A Last access just simply means that that's the last time that file was touched by the system. It doesn't mean it was modified. It just means that file was touched. And that's kind of standard when the system is indexing, or antivirus programs are running, or normal system operations.
Q Are access dates regularly used by forensic examiners?
A No. Access dates are rarely used by forensic examiners, any quality forensic examiners. The reason why is, most of the forensic training classes will tell you that there are too many variables that affect the last access time in order to allow an examiner to form an opinion. As I said, antivirus, other maintenance programs going on.

And so, rarely, do people use last access times. Not only that, but in starting with Windows Vista, Microsoft stopped updating the last access time.

Q Would that be for all models of Windows?

A No.
Q Or just a specific set?
A No. It's generally consumer models. A lot of the professional versions still have last access time, and you can turn it on. You can -- and in Mr. Seleznev's computer, the last access time was enabled.
So, as we saw by the touching of all the last access times, it was enabled in his computer. But in most of our computers today since Windows Vista, other than the Professional versions, that's disabled.
Q After examining all 3300 files, did you draw any conclusions about it?
A Yes. They were consistent with the rest of the evidence on the computers, which these files were accessed as a result of. They correlated with McAfee or SpyHunter or other system type of maintenance operations.
And again, I just want to emphasize. "Last access" just means that, "access." It doesn't mean anything was changed in that file. It just means accessed.
Q Showing you what's been marked as Government's Exhibit 50. Do you recognize this?
A Yes. This is another screenshot of the output of that System Resource Usage Monitor database, that diagnostic-like database. And this particular output is of the application resources.

What's really interesting, if I could say, one of the features of this SRUM database is it's recording how much energy each application is using each hour. So I told you before, it's not only recording how much network bandwidth is coming in and out for each application each hour, but it's also recording the energy usage for each of those applications so we could diagnose, Why is my battery dying so quickly? You can get that information out of the SRUM database.

And it also records which user is responsible for each of those programs or applications that are running. So that's what we're looking at here is the application resource usage.

Q And looking at the --

MR. CHUN: Your Honor, United States moves to admit Government's Exhibit 50.

MS. SCANLAN: No objection.

THE COURT: Admitted.

(Exhibit 50 admitted.)

Q (By Mr. Chun) Looking at the user ID column here, what conclusions do you draw?

A Again, it's consistent with the rest of the evidence on the computer. The last time an application was run that was responsible by a user was the McAfee and -- yeah, McAfee programs. And you can see his user account here again, the smaus user account. And these were the last applications.

Everything after this, you see the security identifier of the system. So this is very consistent with the system doing its normal maintenance and...

Q Now, you heard defense expert state that it would have been impossible for Agent Mills to see the splash screen on August 1st because this laptop was fully off, because it required a full reboot for which there is no evidence of.

Do you agree with that?

A No.

Q Do you agree that there is no evidence of a full reboot on August 1st?

A I completely agree there is no evidence of a full reboot. I think it's already been testified to by the defense experts. There would be hundreds of files that would have been changed. There would have been event logs created. There would have been registry keys updated, if a full reboot occurred.

Q Do you agree it would have been impossible for Agent Mills to see the splash screen on August 1st on this laptop?

A No. It's completely consistent with the evidence that I looked at on the computer.

Q Do you recognize Government's Exhibit 45?

A I do.

Q Did you create this?

A This is a screenshot that I created, yes. Again, the red

boxes are my entries.

Q This is a two-page exhibit?

A Uh-huh.

MR. CHUN: United States moves to admit Exhibit 45.

THE COURT: Any objection?

MS. SCANLAN: No.

THE COURT: Admitted.

(Exhibit 45 admitted.)

Q (By Mr. Chun) Could you please describe what we see here?

A Uh-huh.

This top box here is a screenshot of Mr. Lahman's report where he showed the last entries in the USN journal log. And you can see here that the last entries were the two event logs: the NTFS/operational, and WCM service/operational.

And then I put a red square around the "Report to transfer." This is the Sony Vaio Home Improvement Program. And then below, this is my screenshot showing just the full path so that you can see clearly that this is the Sony Corporation Vaio Improvement file. That was the last thing the USN journal log recorded that was being touched was that Sony Vaio Improvement Program.

Q Going to the second page of this exhibit, could you please describe this?

A This is very similar. This is also on Mr. Lahman's report. This is his screenshot. I took a screenshot of what

he did and added this red box around the configuration file.

This shows the three files that were updated on August 1st. And then below that, you see I did the same thing, just showing the full path of those same three files.

And, again, you can see we have two files here with the extension RSLC. I believe those to be the resiliency files for the metro app. And then you see that configuration file for the Sony Vaio Improvement Program.

Q Seeing that the last three activities were similar to the only three files changed on August 1st, what is your conclusion about this?

A Well, this is consistent with the rest of the evidence on the computer that I examined, as well as Agent Mills' testimony that he saw a splash screen. Because the last thing that the USN journal log recorded was that it was touching and using the Sony Vaio Improvement Program.

And then on August 1st, when Agent Mills said that the computer awoke and he saw a splash screen, it's very consistent that the three files that were updated with the last thing that the computer was doing when it shut down or when it quit.

Q Showing you what has been marked as Government's Exhibit 51. Do you recognize this?

A Yes. This is -- oh. This is the Energy Usage Table in that SRUM report. This is why we get so excited about this

SRUM database is, this is also recording what is the energy level of the battery that's in the laptop.

And if you look along this right-hand side right here, you can actually watch the battery draining. And the last entry in this log, the Energy Usage Table, shows that the battery got to 2.68 percent. And that was recorded on 7/13 at 23:56.

Q And as it drains down to 2.68 percent, what do you believe happened next?

A Well, I believe what happened is, once a computer gets down -- and this particular computer, I believe, was set at two percent. Once the battery level gets to two percent, it basically goes into kind of a -- I don't want to say a panic mode. But it says: I have no more battery. I'm about to run out of battery, so I'm going to stop all my Connective Standby activity. And it goes into what's called a DRIPS state.

Q Can you describe what "DRIPS" is?

A A DRIPS state is a -- D-R-I-P-S. It's something-Resource -- oh. Deepest Runtime Idle Performance [sic] State. Yeah, Deepest Runtime Idle Performance State, DRIPS.

Q Would that be the "Platform State"?

A Yes, Platform State. Thank you.

So in DRIPS mode, what's happening is, in order for a computer -- this just came out in Windows 8, this new feature

of Connected Standby.

In DRIPS mode, what it's doing -- or, first of all, to be Connected-Standby capable, it is a hardware and software requirement. So you have to have a certain type of low-energy or low-power RAM, DRAM.

And you also have to have a system on chip, so your wireless-network card can hold its own state. So if it connects to a network, it can do its own thing. The audio can still play. So it operates like a cell phone. You can receive Skype calls or text messages, even though it appears to be off.

One of the deepest states is the DRIPS, the Deepest Runtime Idle Platform State. And, at this point, it's my belief that all that happened after it reached two percent was it was just trickling the remaining two percent of the battery to the low-power RAM.

Now, DRAM actually holds memory in the cells. I typically refer to them as like little paint cans. And it negatively or positively charges that paint can and closes the lid. And the paint can can only hold that energy for so long before it wears out.

So the DRIPS mode, all that's happening is, it's just kind of pulsating a little tiny bit of energy to RAM to try to help RAM maintain its last state. And I believe that that's what happened once it reached two percent.

Q Did you examine this computer to see if it went into hibernation?
A I did.
Q And what would you look at to check that?
A Well, when a computer goes into -- "hibernation" is a specific term. And when a computer goes into hibernation, on the root of the hard drive there's a file called a "hiberfil.sys."
Q Showing you Government Exhibit 52. Do you recognize that?
A I do.
Q What is that?
A This is a hiberfil.sys right here. If you could zoom into the top here.

MR. CHUN: Move to admit Government's Exhibit 52.

MS. SCANLAN: No objection.

THE COURT: Admitted.

(Exhibit 52 admitted.)

Q (By Mr. Chun) Could you describe what we see here, please?
A If you could zoom into the top where I circled. This is the file, hiberfil.sys. And you see that the last modified time is recorded as June 27.

So it would be very easy far a novice forensic examiner to say: This computer didn't go into hibernation. The last time this hibernation file was used was June 27.

But if you actually look inside -- and if you go back and now zoom in. This is inside the hiberfil. If you look inside -- and I apologize about how technical we're getting. But right here at hex offset 20, that's what I've highlighted. This 8 hexmadecimals, this is a date/timestamp.

Any time your computer starts to go into hibernation mode, the first thing that it does in that hibernation file, on hex offset 20 -- this is on Windows 8, 8.1 -- it writes the date and time that it's trying to go into hibernation. And then it would store all of its RAM on the hard drive in that hibernation file.

Now, I've highlighted that hex offset 20. And if you could back out to the lower left-hand corner, you can use a hex value interpreter. So what I've got highlighted here is the date/timestamp. And you can see that on 7/14, at 12:36 a.m., that date/time was written into the hibernation file.

So I believe what happened, when you take the totality of the evidence here, is that this computer was getting to its last possible battery usage. And it says, I need to go into hibernation, into DRIPS mode. It wrote this file.

If you look through the rest of the hibernation file, it does have some information. But, for the most part, it did not write RAM out completely. Normally, that's what would happen. But we see that it wrote the date in the hibernation file, but that was the last thing it did. It would have

taken too much energy to actually write -- since it only had two percent or less, it would have taken too much energy to write that RAM to the hard drive.

Q So, based on your examination of all these forensic artifacts, what is your conclusion that happened between July 14th and August 1st, and what Agent Mills saw on August 1st?

A Well, based upon my examination and the evidence that I saw of the computer; and reading Agent Mills' statement that he saw the splash screen; looking at the SRUM, that it had reached two percent; looking at that user journal log, that the last thing that it was doing before it lost its power was doing the Sony Vaio update. And the only thing that it did, essentially, when it came to awake on August 1st was finish doing the last thing that it was doing. I believe this thing went into a form of DRIPS where all it was doing was hanging on, trickling that RAM as best it could. It is consistent with the rest of the evidence.

The last thing you see in the user journal log is the Sony Vaio Improvement Program being used. The first thing, when it comes out and wakes up, is a Sony Vaio Home Improvement. If it would have shut down, we would have seen hundreds of files, as previously been testified, showing a boot-up. But we don't see that.

So based on all of that, I think Agent Mills' testimony is -- is exactly accurate. He did see a splash screen. He,

then, killed the computer with the power-off. And all of this is consistent with it being in just that Deepest Runtime Idle Platform State.

Q Now, as part of your work as a forensic examiner, have you conducted a live image of a computer before?

A Oh, yeah, absolutely. Many times.

Q Of RAM?

A Yes.

Q Of a hard drive?

A Yes.

Q And you've dealt with encrypted computers before?

A Yes, unfortunately.

Q When you're dealing with an encrypted computer, what is the importance of conducting a live image?

A If you have a whole-disk encrypted computer and you just power it off, like is kind of the standard operating procedure or the best practice, you push power and kill it, what you now have is a doorstop. If it's a whole-disk encrypted and you don't image RAM, generally speaking, you're not getting into that computer.

So if you have what you believe is a whole-disk encrypted computer, your best chance of getting that data is two things. One, image RAM with the hopes that you can pull the password out of RAM for the encryption; or two, on the live system, image the computer while it's running.

Now, of course, I have to say that in order to image the computer while it's running, it actually has to be in the environment. You can't image a computer if it's been logged out and you're at the lock screen, because you actually have to run your forensic tool on the live system in order to image it live.

And if you image it live at the logical level -- because there's two ways to image a computer: Logically, and that means those files as they exist; and physically, how they sit on the computer.

Even if a hard drive is whole-disk encrypted, once you log in you're not seeing any encrypted files. And the reason why is, because you put in your password and the system is decrypting all those files as they're being presented to you.

So on a live computer when you're in the operating system, if you're using that person's credentials, you can start. As Agent Mills testified, you could plug in a thumb drive, something like FTK Imager. And you could image that computer live at the logical level, and all of those files would be image unencrypted.

Q Would the computer have to have power to do that for a live image?

A Of course. Of course.

Q You need to be powered on?

A Yes.

Q That's what we mean by "live," correct?
A Yes. What we mean by live is not only power, but you have to be in the environment.
Q And so if you have a computer that is on that you would want to live image, would supplying power to it be a justifiable step?
A Sure. It has to be live.
Q And that's so that it would be powered for the live image attempt?
MS. SCANLAN: Objection; leading.
THE COURT: It is leading, counsel.
Q (By Mr. Chun) And what would be the importance of power for conducting a live image?
A You can't image a computer live if it's not live. So it has to have power to be live.
Q Based on your knowledge of this case as a whole, have you reviewed reports and such? Are you familiar with the facts of this case?
A I am.
Q Would you have expected this computer to be encrypted?
A Absolutely. This is what I would consider a high-technology crime, someone stealing credit cards and passwords. So that's an advanced high-technology crime.
So you would expect the person doing it to have an advanced knowledge of security, because you don't want to

steal credit cards and then somebody steal them from you. And you certainly don't what somebody going onto your computer and taking your bounty, so to speak.

So it's completely logical to expect that this computer would be whole-disk encrypted.

Q Now, believing the computer was encrypted, would you have attempted a live image of RAM?

A Absolutely.

Q Now, knowing that the computer had been only on battery power for nearly a month, would you have expected live imaging to work?

A That's kind of a complex question. If I can explain it a little bit.

I'm not sure if I know of a computer that would last 30 days on battery. So what happens typically, when a computer runs out of battery power, is it goes into hibernation mode. And, as I just mentioned about hibernation mode, when it goes into hibernation mode, it takes everything that's in RAM and it writes it to the hard drive in that file that we just looked at called the hiberfil.sys.

Now, if this computer was anticipated to be a whole-disk encrypted and had been in the evidence room for 30 days, the best thought would be the battery ran out. And as the battery ran out, it would have written RAM to hibernation file.

Now, because it is whole-disk encrypted, that's worthless to you, because the hibernation file is inside the whole-disk encrypted computer. So the only way you could have imaged RAM is by applying power to the laptop, bringing it out of hibernation. And when you bring a computer out of the hibernation, it reads out of the hibernation file the RAM that it had, just before it went into hibernation. And now all that information is back in RAM, and at that point you would conduct the image.

I mean, let me be clear. This is like -- this is the Hail Mary. Obviously, my height, I'm not a basketball player. But this is like tossing the basketball from one end of the court to the other. You've got one chance.

If you expect this computer is whole-disk encrypted, if you don't at least try to image it live, you've got nothing, zero. Doing this technique, hoping that it went into hibernation mode, reapplying power and having it come out of hibernation, read that RAM back off the hard drive, it's a Hail Mary. But it's the only chance you got.

Q Showing you what's been marked as Government's Exhibit 43. Do you recognize this?

A Yes. This is the screenshots that I created, I think yesterday or the day before, yes. Yes.

MR. CHUN: United States moves to admit Government's Exhibit 43.

THE COURT: How many pages is that, counsel?

MR. CHUN: It's two pages, Your Honor.

THE COURT: Any objection?

MS. SCANLAN: No, Your Honor.

THE COURT: It's admitted.

(Exhibit 43 admitted.)

Q (By Mr. Chun) What are we seeing here?

A What you're seeing is an excerpt. On the left, this is an excerpt of the USN journal log. This is that flight recorder.

And I specifically filtered out everything except for application event logs, because the defense experts had testified that they saw application event logs in the USN journal log. But then when they examined the actual event log, they didn't see an event written.

And they seem to suggest that that means they, somebody, edited out these entries, because it couldn't be in the journal log saying it wrote to the application event log, if nothing was written to the application of that log.

And this was just an example I was trying to show the prosecutors, that that's just not the case. There are several instances. And this page you're looking at, the application event log, entries in the USN journal.

And on the right-hand side here, you're seeing the actual application event log. And those items on the left,

highlighted in red, show the user journal log saying, I am data overwriting to an event log. And there's many instances where no event log is created.

Q And showing you the second page of that exhibit. What do we see here?

A This is just another example of instances where the USN journal log says that data was being written to a log, and there's no entry in that log. And it was presented before that this is inconsistent Windows behavior. And it's not inconsistent Windows behavior. It happens.

Q On the right-hand side here, these two tabs at the top, what would those be?

A This is the application I was using to review event logs. And I had two event logs open. One was the applications event log, and the other was the security event log.

THE COURT: How much do you have left?

MR. CHUN: One or two, Your Honor.

THE COURT: Go ahead.

Q (By Mr. Chun) Yesterday you heard the defense expert say that, based on the state of this hard drive, that everything on it would be unreliable.

Would you agree with that?

A Absolutely not.

Q And is that based on your review of this exam and all the artifacts it contains -- of this hard drive and the artifacts

it contains?

A Yes. Based on the -- the artifacts are consistent with what happened. Not only that, but we mentioned before, yesterday, that a thing called volume shadow copies. And what -- volume shadow copies are snapshots in time of your computer. And there were multiple volume shadow copies from even before seizure of the computer. So this computer is -- its integrity is intact.

And it's even further verified. You could go back into volume shadow copies from before when the government had access to the computer, and see from those volume shadow copies that this computer is intact.

Q So your opinion is, this hard drive would be reliable?

A Absolutely.

MR. CHUN: No further questions, Your Honor.

THE COURT: We'll take our break now.

(COURT IN RECESS.)

THE COURT: I believe counsel for the government completed examination. We'll move on to cross-examination.

MS. SCANLAN: Thank you, Your Honor. I'm having technical difficulties between my computer and the monitor system.

THE COURT: What does that mean?

MS. SCANLAN: It means, what is on my computer is not on the screen.

THE COURT: We have a number of experts in the courtroom. If they can't help you, you're in real trouble.

MR. CHUN: Your Honor, I apologize, but it comes to my attention that I failed to admit Exhibits 42 and 51. I discussed it with defense counsel, and they have no objection.

THE COURT: Admitted.

MR. CHUN: Thank you, Your Honor.

(Exhibits 42 and 51 admitted.)

CROSS-EXAMINATION

BY MS. SCANLAN:

Q Good afternoon.

A Good afternoon.

Q I wasn't going to start with this, but I'm a little bit afraid not to. We're going to start with what's on your monitor, okay? Exhibit 126.

You testified about the -- what you're calling the DRIPS state, right?

A Yes, ma'am.

Q So when you remount the image into your computer and turn it on, it shows the system shutdown was July 14th, right?

A Well, this is a generated artifact that is not part of the original evidence.

Q Right, I know. But you were saying -- I know that you took this image, right, and you rebooted it?

A Yes. Multiple times.
Q Multiple times?
A Yes.
Q And when you do that, it says the previous shutdown in the system event log was July 14th, right?
A I believe, based on this screenshot. But I did not look at this and I did not conduct that test, because all the other forensic evidence was consistent with it not. So I'm not arguing this.
Q Okay.
A This is what your experts did. I trust your experts that they created this by rebooting the image.
Q Right. Because you spent an enormous amount of time, recently, creating images and doing testing, correct?
A Some time.
Q Right.
THE COURT: One at a time.
Q (By Ms. Scanlan) But you did not just mount the image and take a look and see if this was the last shutdown?
A I did not. I did not look at this event log.
Q If we assume that my experts didn't make up this image, okay, isn't this different than what you're saying about it being in DRIPS state? Because this is telling you it shut down on that day, right?
A Well, this is just an event log saying there was an

unexpected-system shutdown. And we don't know to what extent that unexpected-system shutdown was. If it were to go into hibernation mode, the same thing might have happened.

This event log could be created, perhaps, even if the system doesn't totally shut down, but a portion of the operating system.

Q Just so I understand your testimony, you can have an unexpected shutdown that is actually this hibernation mode?

A I'm not saying that that's what would happen.

Q So that's just a theory?

THE COURT: Okay. Let's not overlap. Let the witness finish and let counsel finish her question.

Next question.

Q (By Ms. Scanlan) What's a "SIM card"?

A A SIM card is typically a -- I forgot what the meaning of SIM card was, but it's basically a little card. You can put them into phones. They can hold data. You can put them into computers. They're like a microflash. They're very tiny. They are about the size of your fingernail and hold data. They can do a number of things.

Q You put it in your phone, right, and it creates some connectivity for you?

A Uh-huh. That's one type of SIM card that you put in your phone for your phone carrier.

Q Okay. And that will -- I know I'm not going to use the

exact words you'd use. But that's how you connect to things?
A Absolutely.
Q So the computers with SIM cards, the SIM card acts in the same way?
A Yeah, I think it acts similarly.
Q I know we just found this out. But prior to 30 minutes ago, did you know there was a SIM card in the Sony Vaio laptop?
A I had a suspicion.
Q Why is that?
A Remember when I told you about the registry keys that keep track of every network that's connected, this computer connects to, how it's connected? You can tell whether it's wired or wireless.

Well, one of the indicators, name types indicates whether it's a 3G connection. And so wireless was 47, wired was 6, and then there's one for 3G connections.

And so I saw in the networks that previously -- I forgot the name of it. But it had the last portion of ROM. There was a network that appeared to have a name type from a network card.
Q Okay. Did you put that in your report?
A No, because it was prior to the computer coming in contact with law enforcement.
Q Well, the SIM card being there wasn't part of that, right?

Just the log that you looked at; is that correct?
A Sorry?
Q Meaning, the SIM card was in the computer when law enforcement had it. You're not saying that it wasn't, right?
A Oh, no, I'm not saying -- I did not know definitively that there was a SIM card until they came in and said something. But when they said something, that triggered my thought: Well, gosh, when I was looking at all of these networks, I did notice one of the networks that it connected to was this ROM.
I've got it written down somewhere, but you can look and see. So it doesn't surprise me that there was a SIM card.
Q Okay. Different topic.
A Okay.
Q When you press down the power button on this laptop to turn it off, what logs are updated?
A How would you press down the button? I'm not trying to be difficult. What I'm saying is, if you just touch the button, that's one type of press. But if you press and hold for ten to 15 seconds, that's a different type of action.
Q I think we're going to go with press and hold.
A Press and hold?
Q Uh-huh.
A Press and hold. I don't know that there -- you're asking what event logs would be updated?

Q Yeah.
A I don't know that any event log would be updated, because that's almost analogous -- pressing and holding the power button is almost analogous to unplugging the battery, all power source.
Q The system log wouldn't log an unexpected shutdown if you did that?
A It may. It very well may.
Q So that's one event log that -- it tends to be updated when you press and hold the power button?
A Actually, that would be created when you rebooted the computer possibly, as your expert showed.
Q The one we were just looking at?
A Yes, ma'am.
Q I know you've been here. You heard Agent Mills talk about the fact that he pressed and held the power button on August 1st?
A Yes.
Q What are the artifacts from him doing that that you see in the image of this computer?
A The only artifacts that I saw, from the image of the computer, were those three files that resumed that were updated that were the last files that were being looked at in the USN journal.
So the Sony Vaio configuration file was updated. But I

didn't see any other logs or files or event logs that were recorded as a result of that kill power.

Q So the system event log didn't record an unexpected shutdown from him holding the power button?

A It was not in the logs that I saw.

THE COURT: Just so I'm clear, counsel. The questions that you asked about holding the power button down was not in the logs was the answer. I want to clarify, are we talking about the push-and-hold or just pushing? Clarify that.

MS. SCANLAN: The push-and-hold.

THE COURT: All the testimony was about push and hold, not just touching?

MS. SCANLAN: That is my understanding of the testimony.

THE WITNESS: I agree. That's what I thought I heard.

THE COURT: Okay. We're clear.

Q (By Ms. Scanlan) You showed us some screenshots of a number of tests where you went to the splash screen, and you indicated that the Winlogon registry key updated?

A Correct.

Q And you had not logged in?

A Correct.

Q The Winlogon registry key has 24 values?

A This particular one did, yes, ma'am.
Q Okay. So I wanted to show you -- can you see that?
A I can.
Q This is Government's Exhibit 42.
A Yes, ma'am.
Q These -- on the right-hand side, the longer list is the 24 values of the Winlogin registry key, right?
A Yes, ma'am.
Q Let's just take a look at -- for the purposes of this, the top one is this "Userinit." And you see the data portion?
A Yes, where it says, "C: Windows directory/System32" --
THE COURT: Repeat that, counsel.
A This is where the data portion says, "C: Windows directory/System32 subdirectory," and then "Userinit.exe." This is fun forensics stuff. I get excited.
Q (By Ms. Scanlan) So take a look at this one, and I'll show it to you again. This is Exhibit 48. This is one of your screenshots, right? Can you see that?
A Yes. This looks like the screenshot from my test on May 24th.
Q And this is when you go to the splash screen, but you don't log in?
A Correct.
Q Did you notice that all 24 values are the exact same as they were on July 7th?

A I did not notice that they were all the same. I don't know that that is true.
Q Do you want to take a minute? I'm not trying to trick you. Can I bring these to you? Do you want to check?
A Sure, if you'd like.
MS. SCANLAN: May I approach?
THE COURT: You may.
THE WITNESS: Thank you.
A Yes, these all look the same. It looks like the values are all the same.
MS. SCANLAN: May I retrieve those, Your Honor?
THE COURT: Yes.
Counsel, it would help the court if you would put them back on the screen and point to where he was looking, to assess the representation.
Q (By Ms. Scanlan) This is Government's Exhibit 42. And we have this section. All of these are the 24 values, correct?
A Yes, ma'am.
Q Okay. Maybe I'll let you draw the line.
A Okay.
Q Exhibit 48. Can you do the same thing, so we can all see which ones are the same?
A Yes, ma'am. These are all the same, these values.
THE COURT: Thank you.
Q (By Ms. Scanlan) Can we talk about shadow copies?

A Sure.
Q Let me just get the number for you. Exhibit 42 is a shadow copy.
MS. SCANLAN: Your Honor, my screen is not currently on, so I can't see it. Should I just hit the power button?
Q (By Ms. Scanlan) Exhibit 42 has more than one page, correct? Do you remember that?
A Yes, ma'am.
Q Let's go to the next page, please. I don't know if you can see this, but the last written date for this one is June 11th?
A Yes, ma'am.
Q So you were mentioning, at the end of your testimony on direct, that one of the things that supports your opinion regarding the reliability of the drive as a whole is the things that you looked at in the shadow copies, correct?
A Correct.
Q And these are part of that, these shadow copies?
A Yes.
Q You were here when Mr. Lahman was asked some questions about these, were you not?
A I was. I don't remember which questions you're talking about, but I was here.
Q Okay. There were questions about -- so if you look at the thing that's in blue with the red box, the shutdown flags?

A Yes.
Q Can you see that?
A I can. Well, it's blurry, but -- oh, there we go. Thank you. Yes.
Q This is one of the things that you indicated -- if I understood correctly about the shadow copies. That this updated the Winlogin registry, this change in the shutdown flag?
A Yes. In looking at those volume shadow copies which are snapshots in time of the computer, this is one of those snapshots in time previously that shows the same Winlogon registry key.

And I drew this red box and highlighted the shutdown flags' value, because that was different than the current state of the computer when we looked at the end.

So the current -- the current operating system is different from the volume shadow copy that we're looking at here of that same registry key. And if you look at a previous volume shadow copy of that, that value is different.
Q Okay. What does that mean?
A I don't know definitively. But, essentially, what it means is that in this volume shadow copy when the computer was shut down, the shutdown flags was a different code than it was the last time it was shut down. So that could mean any number of things.

I don't know definitively what the shutdown flags represent. But, typically, that would suggest to me: How was the computer shut down? Is there anything we need to know when we come back up to do differently? I really don't know exactly what the shutdown flags mean. I'm just guessing.

Q Are the shutdown flags one of the values of the Winlogon registry?

A You have it on the screen here, yes.

Q I do. I'm just not sure it's apparent from the screen.

A Yes. Here's the shutdown flag. It's highlighted in blue.

Q And this is one of the values of the Winlogon registry key?

A It is.

Q And so on this day, are we saying this value changed through system activity?

A Can you zoom into the date? What is the date here?

Q June 11th.

A June 11th. So all we can say from the screenshot is that the value of the shutdown flags, in this Winlogin registry key, was different than the active state of the computer at this date and time.

When the computer made this automatic volume shadow copy, this snapshot in time, this was what the value represented. That's all we can say about this screenshot.

Q Okay. Maybe I misunderstood the questions that were asked of Mr. Lahman then. Because I understood what this was supposed to demonstrate was that system activity updated this value on this day without a login. Is that not what this is showing us?

A I think -- I apologize. I do believe you're misunderstanding.

There were two portions about this Winlogin registry key. One question had to do with, when does the last write time get updated? And in our tests we demonstrated that the last write time gets updated, not necessarily when the user logs in, but when the computer boots up from that restored image. And there was another time, again not logging in, that after 24 hours it updated.

I think the question here is, looking back in time, we can see what values were different from the current value in each of the volume shadow copies.

Q So this had nothing to do with the system actually updating the Winlogin registry?

A We really don't know what updated this shutdown time.

Q Oh, okay.

A As I said, this is an artifact that it's just not normally used in forensics. So we don't know as much about it as we will in the future.

Q Let's take a look at Exhibit 43, if we can. Did you put

these red highlights in?
A I did.
Q What is this telling us?
A I was just highlighting for the prosecutor that, in these instances where the USN journal log -- slow down.
In these entries that are highlighted in red in the USN journal log that show that the application event log had data overwrite, in the corresponding application event log on the right, there were no corresponding events that we could find that match those times.
So this was nothing more than an exhibit to say that the user USN journal log can say there was data overwrite, when, in fact, there is no apparent data overwrite on the file.
Q So the USN journal is the area on the left of the screen?
A Yes, ma'am.
Q And the information on the right is the application event log?
A It is.
Q All the ones in red say "Data overwrite/close," right?
A Yes.
Q And all the ones that are not highlighted just say "Data overwrite"?
A Correct.
Q What is a data overwrite/close -- is file the word, I don't know -- event? What is it?

A What was the question?
Q What is the data overwrite/close?
A It's just an entry that says -- I don't see what the header is.
THE COURT: Counsel, can you expand that?
MR. BARBOSA: Yes, sorry.
A That is just the USN-journal-received reason.
Q (By Ms. Scanlan) What's the difference between data overwrite and data overwrite/close?
A I don't know definitively. I would assume it means it closed the file.
Q But you notice that all the ones where you're saying it doesn't match are all that type, right?
A I do. On this particular event log, I do. But there are other event logs, like the security event log that just says data overwrite and the same anomaly occurs.
Q Okay. This application log -- I'm going to switch you over, so you can see this screen. Can you see that?
A I can.
Q "Can" or "cannot"?
A Yes, I can. Sorry.
Q So you see -- you were here when Mr. Lahman testified about this, right?
A Yes.
Q This is the journal -- the USN journal overwrite changes?

A Yes.
Q And you see that the application log here is -- the reason says data overwrite, right?
A That's correct.
Q And none of these reasons say data overwrite/close, do they?
A Not on the ones that he has highlighted, no.
Q Well, how about the other 12 that are right there?
A On the ones that he is showing, no.
Q And these are the ones that had changes when the Winlogon registry key changes?
A Correct.
Is that what he testified to, that these had changes?
Q Uh-huh.
A But if you look further down that list, there are security event logs that just say data overwrite, just like these, that have no corresponding event login.
Q Okay.
A There are multiple instances of data overwrite where nothing is actually written into the log.
Q When we're looking at this USN journal screenshot for July 7th, this number 7 is a security event log, right?
A Correct.
Q And it says "data overwrite"?
A Correct.

Q It doesn't say "data overwrite/close"?
A Correct.
But this is just a fraction of the instances of the security event log that the defense expert chose to show, because it matched his theory.
If he would have showed all of them and checked each security event log with the actual security event log, he, too, would have found there were instances where the user journal log said data overwritten, not data overwritten/close and there is no event log.
Q And, likewise, if you had chosen to take a look at the hash values for the Windows registry login on July 7 versus the screenshot tests that you ran, you would have seen they were the same. But you didn't, right?
A I don't follow the question. Which hash value are you talking about?
Q We're talking about the thing that we looked at at the beginning, the 24 hash values that are exactly the same.
A Oh. Registry values.
Q Registry values. They are exactly the same, right?
A Yes.
Q But you didn't compare them before today?
A I --
Q No?
A I did look at them, yes.

Q Now I'm confused. But did you know they were the same?
A I believe I did.
Q You did?
A Yes, I believe I did.
Q Okay. So if the Winlogin registry key updates when you just go to the splash screen, did we see an update when Agent Mills saw the splash screen?
MR. CHUN: Your Honor, objection; vague as to when Agent Mills saw the splash screen.
THE COURT: I think there's only testimony of one specific time that Agent Mills saw the splash screen.
MR. CHUN: There are two instances, Your Honor.
THE COURT: One on the plane and one in the lab?
MR. CHUN: No, Your Honor. Agent Mills would have seen it in the vault on July 9 and then again on the 1st.
MS. SCANLAN: I can clarify.
Q (By Ms. Scanlan) What I'm talking about is on August 1st, 2014, Agent Mills is now reporting that he saw a splash screen come up on the Sony Vaio, correct?
A Correct.
Q And you're saying that when you see the splash screen, the Winlogin registry key updates; yes?
A Partially, yes. What I did was boot the computer, so I restored the image and boot. And during a full boot, it actually got -- the Winlogin registry key got updated.

So when you do a full boot of a restored image from Mr. Seleznev's computer, that registry key gets updated. But our belief and the evidence shows that it did not go through a full boot when Agent Mills saw the splash screen. Hence, that's why you don't have that updated registry key.

Q So then you did an experiment where you didn't have it go through the full boot, and you looked to see if Windows registry key updated?

A Yes.

Q Did it update?

A Not consistently.

On one instance when we left it overnight -- because we did a very series of tests. Sometimes it was one hour that we left it, it didn't update. Two hours we left it, it didn't update. Twenty-four hours we left it at the splash screen, and it did update.

So, again, this key is not designed to record when a user logs in. It's inconsistent in when that registry key gets updated.

Q But when it gets updated from the splash screen --

A It doesn't get updated from the splash screen.

Q Sorry. It updates when the splash screen comes up?

A No, ma'am. It updates when you start the computer.

Q Okay. Sometimes?

A Sometimes.

Q I just wanted to check. I know that we're talking about the DRIPS state. But after July 14th, there is no USN journal activity; is that correct?
A Correct.
Q You were talking about antivirus activity and access dates and modification dates. Do you remember that?
A Yes, I do.
Q When antivirus sweeps through a computer, in this case, you're saying it only touched these 3300 access date files and 274 modification files during that whole time period?
A Well, that's all that we see.
Q That's kind of a small number compared to the total number of files on the computer?
A I would agree.
Q And so it's a coincidence that some of these files that are touched actually contain this stuff that's of interest to the investigation?
A I don't agree with that, the files that were touched were not what was of interest. If you could explain which files you're referring to, I can better answer the question.
Q Okay. So, for instance, there was a -- I'm going to have to pull it up for you. There was a discovery dump Word file that we looked at with Mr. Blank. Were you here of that?
A I was.
Q And that was one of the files that was in the jump folder?

A I -- I sincerely apologize. "Jump" and "recent" are two totally different forensic artifacts. It was in the recent directory. It was a link file, not a jump folder.

Q And it had an access date that was modified after July 5th?

A Yes. I believe all the link filings seemed to have access dates after July 5th.

Q And that discovery dump file is something that's of interest in this case?

A Well, it's the discovery dump file that's of interest. The link file itself only had a last access date that was updated. The link file is actually a forensic artifact that records generally the first time that document was open and the last time that document was open.

Now, there is a duplicative forensic artifact that corroborates link files that is, in fact, a jump list. Now, a jump list is -- there are two types of jump lists. There is a thing called auto destinations and custom destinations, and those are by application.

So inside those automatic destinations directory, which is in the recent folder, are the jump lists for the applications. And if you looked at the Word "jump list," inside that would be up to a thousand of the last files that was accessed by Microsoft Word, that version of Microsoft Word. This will corroborate the link file.

Again, just another artifact that says, even though the last access time was contemplated, the content of the linked file was not. Otherwise, the modified time would be updated.

Q Are we still talking about my question?

A And the corresponding jump list would also show that same activity.

Q Okay. Was that in response to my question?

A Yes.

Q Let's talk about the last access dates.

A Okay.

Q You said last access dates are rarely used by forensic examiners, correct?

A Correct.

Q Are they used or significant in child-pornography cases?

A Generally speaking, the last access date is not something that forensic examiners use. They want to prove whether the file was actually opened and viewed. So the last access date is irrelevant to that. Because as we saw here, system activities, not necessarily user activities, updates the last access date.

Q So the last access dates are not significant at all in child-pornography cases?

A Generally speaking, they do not refer to the last access date. A good examiner will only refer to the creation and modified dates and those other artifacts that we've been

talking about, such as link files and jump lists.
Q You indicate that, essentially, computers -- to paraphrase, and I'm sure you'll correct me -- don't have access dates updated anymore.
A On many of the versions of Windows, starting with Windows Vista, Microsoft disabled last access update.
Q But not for the Office Suite, right?
A Office Suite is an application, not an operating system. So Vista operating system, the last access date is turned off. It is not on by default. It does not even have the registry key to cause that to happen.
Q For instance, Microsoft Word, the file still has last access dates, correct?
A I truly am not being difficult. Microsoft Word is an application.
Q Right.
A So are you talking about the files that they access, the Word documents that they open?
Q Yeah.
A Whether or not they have last access date is irrelevant. It is whether it's a modified or creation time, because the last access time does not attribute activity to a user. It just says, that file was touched.
Q That's not what I'm asking.
I'm asking you --

A Yes.
Q -- the Office Suites, if you have a file that's part of Office Suite, does its last access date still update on these systems? Yes or no.
A It's not a yes-or-no question.
The Microsoft Office Suite has nothing to do with last access times. What updates the last access time is the operating system, not the application.
Q Okay. I understood your explanation about live imaging and, if a computer was on, you would provide power. That makes sense. But you could do the live image, right?
A Yes, ma'am.
Q You were here when Agent Mills said that he thought the computer was off on July 30th?
A I was.
Q So while it makes sense to you that you would do a live imaging for a computer that you know is on, I'm assuming it doesn't make sense to you that if you thought it was off, you would plug it in to do this live image?
A No, it makes sense.
Q Still makes sense?
A Sure. Because, as I said, if you thought the computer was off as a result of the battery drain of it being in the evidence room for 30 days, the likely assumption is that it went into hibernation mode. And if you applied power and it

was brought out of hibernation, the hibernation file, which contains the RAM, would be read back into RAM. And, therefore, you'd be able to image RAM.

Q And Agent Mills testified that that's what he thought, right?

A I don't recall -- I don't think so. I don't recall Agent Mills saying that.

Q That's what you would think, right?

A Yes.

Q But you don't actually know whether he had all of this knowledge you have about battery --

MR. CHUN: Objection; calls for speculation.

THE COURT: That's sustained, counsel.

Q (By Ms. Scanlan) Do you agree with the evidentiary practice of not signing in and out of vault logs?

A No.

MS. SCANLAN: May I have one moment?

THE COURT: You may. Let's do a stretch break.

MS. SCANLAN: I have no further questions, Your Honor.

THE COURT: Thank you. Redirect?

MR. CHUN: Briefly, Your Honor.

REDIRECT EXAMINATION

BY MR. CHUN:

Q Mr. Carroll, would knowing there is a SIM card in this

laptop change your opinion on the last network connection?
A No, not at all.
Q Showing you Government's Exhibit 44. In regards to your statement --
A Sorry. I don't see anything.
Q In regards to your statement just now about a SIM card not changing your opinion, why not?
A Well, again, there are several artifacts that record any time a network is connected to, regardless of how it is connected to.

There are several event logs or registry keys that will show that. And there is just no evidence on this computer that suggests that it connected to any network after July 5th.

Q Showing you Government Exhibit 34. Do you recognize this?
A Yes. Yes. This is the exhibit that I created or the screenshot that I did of the security event logs as -- excuse me, I apologize.

On the left is the USN journal showing the security event logs. And on the right is a screenshot of the security event logs.

MR. CHUN: Move to admit Government's Exhibit 44.
MS. SCANLAN: No objection.
THE COURT: 44 is admitted.
(Exhibit 44 admitted.)

Q (By Mr. Chun) Earlier from defense counsel, you got questions about how all the red had "Data overwrite/close" in a prior exhibit. Do you see where it just says "Data overwrite only" here?

A Yes. Right here is just one of the instances.

Q Why did you highlight that in red?

A I was just trying to bring the prosecution's attention to the fact that just because you have a data overwrite or a data overwrite/close in the USN journal, and no corresponding event log entered, is not inconsistent with Windows operating system.

MR. CHUN: No further questions.

THE COURT: Anything further, counsel?

MS. SCANLAN: No, Your Honor.

THE COURT: Any objection to this witness being excused by the government?

MR. BARBOSA: Your Honor, we would like him retained, depending on whether the defense is calling any additional witnesses.

MS. SCANLAN: We have no further witnesses.

THE COURT: You may step down, but you are not excused.

MR. BARBOSA: In light of no additional witnesses and no rebuttal --

THE COURT: I want to clarify one thing. The court

had told Mr. Browne that I wasn't going to allow a witness who had been excused to testify. That was prior to the government asking the question about the SIM card. The government only disclosed the information about the SIM card after the break.

Under those circumstances, it would be unfair for the court to preclude from allowing the defense to ask a question about the SIM card. So I'm going to allow the defense to ask only the questions, if you wish to have Mr. Blank, I believe, testify about the SIM card and whether or not that changes his opinion. Because that's the only thing that's different from what we had before.

MS. SCANLAN: Your Honor, frankly, in the last 20 minutes, I forgot about the SIM card. We would ask for the opportunity to do two things.

One would be to ask Agent Mills about the SIM card, since he is the one who just found it. And the second would be to potentially have Mr. Blank testify about whether that changes his opinion. But I do need to speak with him about that first.

THE COURT: All right. Is Agent Mills here? Counsel, is there some particular order preference to have the witnesses testify about the SIM card?

MS. SCANLAN: Agent Mills would be the first to testify.

THE COURT: Sir, please step forward. Agent, you were previously excused. The court will, therefore, place you under oath once again.

DAVID MILLS, HAVING BEEN FIRST DULY SWORN, TESTIFIED AS FOLLOWS:

MS. SCANLAN: Your Honor, the government just handed me the report that Agent Mills just wrote about this. And I haven't had a chance to read it. May I take a look at it before he testifies?

THE COURT: You may.

DIRECT EXAMINATION

BY MS. SCANLAN:

Q Good afternoon.

So I understand you went back to the Seattle field office and took a look at the Sony Vaio, as you've testified?

A Yes.

Q And you located a SIM card in it?

A Yes.

Q I know you brought Exhibit 1, the laptop. Can you show us where that was?

A Sure. It's located on the rear panel of the front screen, a small slot.

MS. SCANLAN: Your Honor, may I approach?

THE COURT: You may.

Q (By Ms. Scanlan) Can you just -- if it's all right, can

you keep it in that state?
A Sure.
Q On the -- you were indicating that on the back cover above the stand for the screen, there's a tiny slot where a SIM card was inserted; is that correct?
A Yes.
Q And there is an arrow that points to that slot pointed on the back of the computer?
A Yes.
Q This is the first time you noticed that there was an arrow on the back of it?
A Yes.
Q And in there was a SIM card?
A Yes.
Q Now, we talked about this with Mr. Carroll, if you weren't here. But it might be helpful, actually, if you could tell us what a SIM card does.
A A SIM card is basically an identification device that will enable a mobile device or a computer to connect to a cellular network.
Q A cellular network. So that's -- we have wireless networks, right, and then cellular networks?
A Correct. So if you're referring to a wireless network, it would be a localized network Wi-Fi. And then we have a wider cellular network, also known as WAN, W-A-N, or a wireless --

or a wide-area network.

Q So just so we're clear. For instance, the way it makes sense to me, if I have a tablet like an iPad, I can connect to wireless networks that are available generally, right?

A Correct.

Q And I can subscribe to 3G or 4G, just like your phone, to have cellular data on my iPad?

A Correct.

Q And that's the SIM card thing?

A Correct.

Q So like a phone or an iPad, this thing has this capability through the SIM card?

A It appears that it does, yes.

Q If you had looked in the arrow slot previous to today, would you have handled this computer in the same way?

A No, not necessarily.

Because I know that, through experience with other devices with this type of SIM card, that you have -- the user has to manually choose to link up to that cellular network versus staying on Wi-Fi. So I probably wouldn't have been necessarily worried about it at that time.

Q Okay. So the fact that it has cellular-connectivity capability would not concern you?

A Not at that time that we received it in evidence, no.

Q Even though, at that point, you knew that it was

essentially on or in sleep mode?
A Correct.
Because, again, through my experience and training, I know that it is customary for a user to actually interface with the device to actually hook up to a Wi-Fi and a cellular network, too.
Q So how do you know it wasn't connected to a cellular network?
A Since it was asleep or appeared to be asleep, I -- I know that, through my experience, that a device just cannot automatically connect to a network by itself.
Q Right. But if it's connected already to a cellular network, you wouldn't have known that, right?
A Not at the time it was received in our office, no. But my experience is that it wouldn't have been able to do that since nobody manipulated the machine previously, logged on and signed into the network.
Q So any computer that's in sleep mode cannot be connected to a cellular network?
A No, not necessarily. If the user has interface with a device and he's connected to a previous network in the area, it's possible through these new operating systems that it could stay connected to that network.
Q You didn't know whether this laptop had ever been in this area before, did you?

A Yeah, I knew that it transited from the Maldives to Guam and then to Seattle.
Q So you knew that that computer had never been in Seattle before?
A I was pretty sure that it hadn't been.
Q Okay.
MS. SCANLAN: Your Honor, may I have just one second?
THE COURT: You may.
Q (By Ms. Scanlan) Is that SIM card associated with any particular carrier?
A I haven't had time to research that. It does have some writing on the back of it and a logo, but I haven't had time to associate that with any known network.
Q So you don't know, for instance, if it had like -- what's an example? Well, Verizon. So if you have a trusted network like Verizon, then it connects as you go, right, like a cell phone?
A Well, again, I think it has to be initiated by the user. Any connection -- or switch from Wi-Fi to the cellular data card has to be initiated by the user themselves.
Q Okay. I just want to make sure I understand.
A Sure.
Q So if you have a cell phone and it's not on wireless, it's on 3G or 4G, same cellular connectivity, right? And you -- it's in its sleep mode and you travel around. It's still

connecting to all the different wireless towers, right?
A Well, it may reach out to wireless towers on other networks and may, what we call, ping them or contact them. But it may not necessarily connect. That requires either an additional subscription or feature initiated by the user.
Q Because we have all these cases where we track people coming down the road, even though their phone is on, but it's in sleep mode because it's pinging. Do you know what I'm talking about?
A Yes.
Q So the SIM card can do the same thing, right?
A Well, in this particular device, it behaves probably in a different manner. It wouldn't constantly connect like a cellular phone.
Q Do you know that, or is that what you --
A Through my experience, that's what I believe the difference would be between this device and the cellular phone.
Q Okay. Is this SIM card -- the way that this is when it's in sleep mode is the way it's connected to standby?
A Say again. Can you say the question again?
Q What does Connected Standby have to do with a SIM card?
A I'm not sure how Connected Standby would actually function with this particular device, since I'm not that familiar with it. I just couldn't tell you what the functionality would be

between the Connected Standby and the SIM card.

MS. SCANLAN: I have no further questions.

THE COURT: Counsel for the government?

CROSS-EXAMINATION

BY MR. CHUN:

Q Agent Mills, prior to this hearing, were you present when defense expert came over and handled that at the Secret Service field office?

A Yes.

Q And did they have an opportunity to pick it up and look at it?

A Yes.

Q What language is on that SIM card?

A I believe it was a Cyrillic alphabet. So I'm assuming it is Russian.

MR. CHUN: No further questions, Your Honor.

THE COURT: Redirect?

MS. SCANLAN: I have nothing further.

THE COURT: Okay. You may step down, sir.

THE WITNESS: Thank you.

THE COURT: Counsel, anything else?

MS. SCANLAN: Your Honor, I haven't spoken to Mr. Blank about this issue at all since it came up. May I have ten minutes?

THE COURT: Counsel, I'll tell you, you reserved two

days for the proceeding. The court is trying to use every minute efficiently.

I know I used a half an hour this morning, so I expect to go a half an hour this afternoon. But I'm concerned about time that we have.

Do you intend to argument on this motion? The court has a calendar tomorrow that's jam-packed. We have seven proceedings starting at 9:00 and going to 4:00 or 5:00. So we obviously can't accommodate anybody on Friday.

So please be mindful of the court's time. Speak with your expert. We'll be in recess.

(COURT IN RECESS.)

MS. SCANLAN: Your Honor, with the court's permission, the defense calls Eric Blank.

THE COURT: Please take the witness stand, sir. I will place you under oath once again.

ERIC BLANK, HAVING BEEN FIRST DULY SWORN, TESTIFIED AS FOLLOWS:

THE COURT: You may inquire.

DIRECT EXAMINATION

BY MS. SCANLAN:

Q Did you learn for the first time today that the Sony Vaio had a SIM card?

A Yes.

Q What does that mean to you?

A Well, now that I know that, I would say it changes my opinions to some extent.

Q In what way?

A Well, I think I would lead off by saying the presence of a SIM card, together with a Windows 8 logo, should have been an immediate warning in July of 2014 that this computer probably had Connected Standby, which came with Windows 8.

And that Connected Standby meant the computer is meant to act like a phone. Meaning, you could travel around through trusted networks, much the way we would drive from here to Spokane, and our cell phones don't use connectivity even though they jump from tower to tower.

At this point, I don't know the SIM card. But I would expect that if it's a SIM card you would get in Russia, it's going to be associated with a Russian telecommunications carrier who have reciprocal agreements with U.S. carriers.

So just as if you're in India and you come to the United States, or if you're in Germany and you come to the United States, your phone still works. And I would expect this Connected Standby feature to work, really, anywhere including in Seattle, Washington.

Q Did you hear Agent Mills say that it would have to be a trusted network in Seattle or a network you had already connected to?

A Right, and I would so agree with that. Except now,

"trusted network" means your phone carrier or a company such as Verizon who has a reciprocal relationship or roaming relationship with your carrier.

So, suddenly, a number of trusted networks aren't just places you've logged on to before, but thousands of networks associated with your phone company or with other phone companies that your phone company has relationships with.

You travel around -- well, I guess I said that already.

Q (By Ms. Scanlan) Is it correct that in order to connect through this cellular network, you have to log on or activate into it when you move around?

A No. That is -- that is what -- so I discussed yesterday, there is standby or what we call sleep, and then there is Connected Standby.

Connected Standby is a computer that is what we call sleeping, that periodically, once a minute -- it is a firmware question -- it checks rundown timers to see if it can make a connection, and it's trying all the time to connect to wherever you take that thing. It is trying to make a connection and connect to the world. And once it connects to the world, then anything can happen to the computer.

And I'm not -- I'm not -- I don't -- it doesn't make me feel any better that the log date on this computer, in a really big case like this, doesn't seem to reflect that kind

of connection. Because these logs would actually be very easy to change.

Let's remember, we're not talking about pulling logs out of thousands of pages of logs. These kinds of log entries we're talking about are happening at the end of this computer's life. The last of any entry is July 14th.

So we're only talking about log entries that were put in place in the last portion of this computer's active life, not in the middle or going to reach back two years and trying to put in sequence numbers.

So the idea that -- I guess, I said in my report. Look, Connected Standby-type features have been available since 2008. It's not a new thing in 2014. It is new with Windows 8 that it comes setup with Connected Standby. But this is not new in the computer-forensics' world.

If you see a computer that you suspect might be able to connect, treat it like you would a phone. And the best way I could put that is, look, the other devices such as the iPad that can be treated like a phone, they were treated apparently the right way. How can you not treat this computer, as if it's trying to connect all the time? And now the chance of it having connected have increased exponentially.

Q You heard Mr. Carroll testify that he thought maybe it had a SIM card, right?

A Right. Yes.
Q And he, I believe, indicated that there was -- he wasn't worried about that, because it looked like those logs for that kind of connectivity did not show a connection in the relevant time period. Do you remember that?
A Yes.
Q So are you saying that it's still possible it connected, even though it's not in that log?
A Yes. We all use logs, but they are diagnostic tools. They're not infallible. It's not that they can't be changed.

It's not -- think of all the investigations that we would never do if we could just say, oh, the system event log shows no connection. So why do we even look any further? So the reason we look further is because logs can be changed. They can be deleted.

And is it farfetched, in this case especially, to think that something like that might be going on? Not at all.
Q So just to sort of tie this back to everything we were talking about before. When you're handling a computer with Connective Standby and with cellular capability like this, is it a best-forensic practice to leave it on for 23 days?
A No, it is not.

MS. SCANLAN: I have nothing further.

THE COURT: Cross?

CROSS-EXAMINATION

BY MR. CHUN:

Q Your super-hacker theory aside, if this computer connected to a cellular network, Windows would have logged it, right?

A I would assume so, yes.

Q And you saw no evidence of that, did you?

A I guess I will say, I've seen a lot of evidence that there are inconsistent logs all through this machine.

Q I'll ask it again. You saw no evidence of a cellular connection to the computer, did you?

A I've seen no log that says I connected to a cellular system. No, I haven't, not after July 5th.

MR. CHUN: No further questions, Your Honor.

THE COURT: Ms. Scanlan, anything further with this witness?

MS. SCANLAN: No, Your Honor.

THE COURT: Any objection to this witness being excused at this point?

MS. SCANLAN: No, Your Honor.

MR. BARBOSA: No, Your Honor.

THE COURT: Does that complete the rebuttal testimony of the defense?

MS. SCANLAN: Yes, Your Honor.

THE COURT: Any additional testimony or evidence on behalf of the government?

MR. BARBOSA: No, Your Honor.

THE COURT: Counsel, how much time did the government believe that you'll need for closing remarks?

MR. BARBOSA: About 15 minutes. I believe Ms. Scanlan and Mr. Browne are going to go first.

THE COURT: Counsel, how much time do you need?

MR. BROWNE: Ten minutes. Well, let me speak to the boss for a minute.

THE COURT: That's on the record, Mr. Browne. The firm name will be changing too.

MS. SCANLAN: 15 to 20 minutes.

MR. BROWNE: Your Honor, sorry. I think a total of 25 minutes. So I don't know how we're going to do that, but whatever you want to do.

THE COURT: All right. Let's proceed.

MR. BROWNE: Continue?

THE COURT: Yes.

DEFENDANT'S CLOSING ARGUMENT

MR. BROWNE: Your Honor, I'm going to confine my remarks to our motions to suppress because of two reasons, the staleness -- because they kind of overlap. The staleness of the information that was utilized in the affidavit for probable cause, one issue. I don't know if the right word is "staleness." The delay is a better word. The delay in waiting for 26 days or more to obtain a search warrant for the computer.

And I know you -- so I know you've read the briefs. And I think the briefs are fairly exhaustive, so I don't plan on wasting a lot of time on it. But I would like to point out some things.

First of all, the first ground, in our opinion, the affidavit submitted in support of the application to search the laptop relied on stale information that fails to establish probable cause to search the laptop.

Two, the 23-day delay in applying for a warrant to search the laptop was, under the circumstances of this case, an unwarranted delay that prejudiced the rights of Mr. Seleznev by creating an opportunity, which we've now seen demonstrated, for the data on the laptop to be altered.

I'd like to parenthetically mention to the court, as far as the second issue is concerned, if -- and I believe it's an "if," and I'll get to that in a minute. If the government had probable cause to -- I hate to use the word "arrest," since it really wouldn't apply in this case.

But if the United States government had probable cause to nab Mr. Seleznev from the Maldives islands and they now claim they have a warrant, which I believe is true. I do not believe, by the way -- because I've done work on this in other cases recently. There is no such thing as an Interpol warrant. So to the extent they relied on that, it's not true. There's no such thing as an Interpol warrant. There's

an Interpol Red Notice, which doesn't give anybody any authority to do anything.

But, in any event, the point I'm trying to make is, if the government believes there was probable cause to arrest Mr. Seleznev -- I will use that word -- then probable cause is probable cause. And this is where we get into some real interesting factors from the standpoint of the time delays.

The probable cause to arrest Mr. Seleznev, then it would follow that they would have probable cause at that time or, perhaps, within a few days to search -- excuse me, to apply for a search warrant to search his computer.

I would say, parenthetically, I'm not sure what authority the government has to take the computer to begin with. How many times have we learned recently, with a computer or an electronic device, you need a search warrant to get it and you need a search warrant to look at it? Here, they just took it. So then they're playing catch-up.

So what they do now is they attempt to get a search warrant to look into a device that they had, in my humble opinion, illegally taken. It's not like a gun. It's not like two kilos of cocaine.

Thank goodness, our courts are recognizing more and more and more again, our electronic devices are our journals of our life. So there is heightened security when it comes to the judicial analysis of obtaining the journals of our lives.

Third, the laptop was so mishandled by the United States Secret Service during the 23-day period from when it was seized and imaged, whether intentionally or it's a consequence of gross incompetence, all the evidence obtained from the laptop should be excluded.

I have noticed, and will relate to you in a moment, this investigation, according to the government's own application for the search warrant -- which I'll be referring to more so than my brief actually, because I think it helps us more. The timeline in this case is interesting.

The United States Office of Secret Service began investigating this case in 2010. At that time in 2010, which is, as we all know, six years ago or more, they developed the name of a nic named "Track2." There is no information about when that nic was officially attributed to Mr. Seleznev, or whether even now they knew that.

They make conclusory -- and I'm going after the affidavit, obviously. That's what we're doing. They make conclusory statements, backed up with nothing, that network intrusions or computer hacks at over 100 businesses between 2009 and 2011 are somehow attributable to Mr. Seleznev. What's interesting about that is, now we're not talking about 2010. We're talking about 2009.

The affidavit for -- you know all the law that we need is in our brief. So I'm going to be talking about the facts of

the affidavit at this point.

We know, on July 5th, 2014, Mr. Seleznev was taken by the United States government from the Republic of the Maldives -- I'll emphasize the word "Republic" of the Maldives -- at the request of the United States government. And he was expelled, according to the government, because of an Interpol Red Notice.

And you can take judicial notice -- I just researched this for anther case -- there is no official ability for any country to act on an Interpol Red Notice. It is simply a notice. It's saying, This person is of interest to us. There is no warrant. There is no nothing.

So in the affidavit, it goes on to say -- and I think these words are really important, because I don't see them much in the search warrant affidavits. Although the crimes in the Indictment occurred between 2009 and 2011 -- this is from the search warrant affidavit -- Secret Service believes Seleznev has been active in the credit card fraud community for several years prior to the crimes in the Indictment. Talk about a conclusion. And that he remained active in the carding community up to his arrest, if we can call it that.

And this is critical. And may -- this is in the affidavit for the search warrant. And may have been responsible for operating new carding websites. "May have." Agents believe that after 2011, Mr. Seleznev, once again, may have adopted a

new online nic, 2Pac. No justification for that statement whatsoever. The same paragraph uses the word "may" six times. Therefore, evidence of his involvement in these new crimes may be located on the subject devices. "May be."

So let's go to the first date mentioned in this affidavit for a search warrant, which we're attacking, is actually February 13th of 2007. So now we're going back even nine years. And that in 2010, a detective named Dunn, who we've heard some testimony about, established an undercover account with a website, 2010.

Rather than go through this, because it would take way too long, I have done -- excuse me one moment, Your Honor. The dates in the affidavit for the search warrant, there are only two mentions of the date 2014, and both of those dates relate to Mr. Seleznev's apprehension. There are 30 dates that precede that. There are seven that are from 2007 to 2011. There are nine that are from 2011 to 2013. That's stale. That's staleness.

We've cited you cases where the Ninth Circuit particular -- and, in particular, relating to personal devices such as cell phones and computers, have said that there's an urgency that keeping these from our possession is like keeping our own personal home journals. Or I like to think about it as photograph albums, or as my mom used to keep albums of current events. So it would be hard-pressed

for me to find a case that I've been involved with that is this stale.

Perhaps, counsel suggests that, well, Mr. Seleznev -- well, first of all, we know he was in a terrorist bombing. You know about that. And he was severely injured and almost died. That was in 2011. Since then, the government tries to argue that because he was injured severely, and the words they used gravely, he was flown to Moscow and survived.

That there was a period of time that lapsed when some of these nics were not being used. What does that mean? It means nothing. Because in the same paragraph in the search warrant affidavit, it talks about how someone else, while he's been recovering in the hospital, has been using those nics and using the websites.

So it would be hard-pressed for me to imagine a case that's more stale than this one. When you go through this search warrant affidavit and there's only three times they mention 2014, and two of them are because of his apprehension, and the remaining 35 are from 2007 to 2011, how can anything be more stale than that?

Now, next argument. Keeping it for 23 days without getting a search warrant. The cases that we've cited to you, Ninth Circuit cases, very recent Ninth Circuit cases, once again, talks about the sanctity of these devices and that the government cannot simply take their time.

If they have probable cause to, I'll use the word, arrest Mr. Seleznev in the Maldives, then they had probable cause, most likely, to get a search warrant. The delay here is unexplainable and has been unexplained.

Now, I think that the agents did a good job trying to protect the integrity of this device, but I do not think they did a good job doing that as quickly as possible. Frankly, I think we're probably all shocked today to learn -- and I want to credit Agent Mills directly for his honesty and his integrity.

And it reminds me of another case that I had where something like this happened, where a young prosecutor told me about something that hurt his case a lot and resulted in a dismissal of that case. So I think the fact that Agent Mills actually found this SIM card, it's almost too far to say it's a house of cards right now, SIM cards included.

I could see the SIM card port on that computer from sitting where I was sitting. We just find out about it today? And we all know enough -- at least I know SIM cards contain information. We don't know what's on there.

So that part of this investigation certainly has fallen short. I don't see any justification for the 23-day delay between -- and I use this word advisedly -- stealing Mr. Seleznev's computer. They had no authority to take it. It certainly wasn't contraband on its face until we've gotten

here.

So I know time is really precious, and I want to thank you for your patience. Would you like me to answer any questions?

THE COURT: No, thank you.

MR. BROWNE: Thank you, Your Honor.

THE COURT: Ms. Scanlan?

MS. SCANLAN: There are -- as the court is aware, there are two grounds that the defense has raised in regards to how the laptop was handled and why this piece of evidence should be suppressed. The first is what we are saying is a warrantless search on July 7th of 2014.

The second is the mishandling of the computer from the time it was seized through the time that it was imaged. It's that second issue that I would like to start with.

There are different levels of messing up or misconduct or not doing something correctly. So, for instance, in *United States v. Flyer,* the agent in that case did not connect the write blocker correctly and there were files that had changed access dates. The defense moved to suppress. The defense moved to dismiss, and the court said no.

I will note it's interesting, however, that the issue in that case was access dates, not modification dates, not creation dates, but these access dates that Mr. Carroll tells us are irrelevant.

Because, in *Flyer*, in this circuit, the government voluntarily dismissed a count where the access date had been changed. It was a child-pornography case. One of the access dates for a piece of evidence that was the basis for a count of possession or transportation of child pornography, one of the two, the file itself had a changed access date because of the agent conduct.

The court in that case noted, in denying the motion to dismiss and in the suppression issue, that the government had already dismissed the count where the access date had been changed.

So it appears, at least from where I'm standing, that this new idea that access dates have absolutely no meaning certainly didn't apply when the government made a decision to dismiss the count in *Flyer*, and it didn't apply when the Ninth Circuit evaluated that behavior. That's not that long ago.

Access dates have meaning. Now, maybe they are not the crucible of file activity or the only thing that we look at. But, really, nobody has said that they are, just that they matter and that it matters when you let a computer in your custody have access dates change while you have it.

THE COURT: Let me ask you a question, counsel. In the *Flyer* case, as I recall reading it, there wasn't a detailed record that was provided in terms of the overall

analysis of what was going on in the government's rationale to dismiss in terms of anything specific. And I don't recall that the record detailed the aspects of computer analysis, as has been done with the testimony of the experts today.

Would you agree?

MS. SCANLAN: Sorry, Your Honor?

THE COURT: In other words, in the *Flyer* case, the government dismissed it before it got to court, correct?

MS. SCANLAN: To be honest, I can't tell whether they dismissed before the initial trial or the suppression hearing or not.

THE COURT: My point is, it's difficult to find exactly what *Flyer* stands for, because there was no analysis of what happened with the computer as we have here today. We have duelling experts here in this case. There's no evidence in the *Flyer* case, no duelling experts, or in the analysis at all about what happened or not. So I don't know if we have enough evidence or facts or analysis from *Flyer* to make it applicable to the facts.

If you can convince me otherwise and point to somewhere in that case where it shows where the court was looking at what factors that they considered in making that determination, that would be helpful to the court.

MS. SCANLAN: Your Honor, the trial court or the Ninth Circuit?

THE COURT: Ninth Circuit.

MS. SCANLAN: I will agree that the application of a suppression analysis by the Ninth Circuit in *Flyer* is limited to about a paragraph and a half.

THE COURT: That's my point.

MS. SCANLAN: The rest of it is a due-process dismissal analysis.

I will say that, for the purposes of my primary point in citing the *Flyer* case, that the *Flyer* case does lay out -- and I admit, at least for me, I had to read it four or five times to get the scenario correct of what happened with the laptop. But there was a defense expert in that case, a government expert. The defense expert, like here, similar, got the image and discovered that all the access dates had been changed. In that case, the government agreed that the access dates had been changed, that they were different.

What is missing from *Flyer* is, after the government dismissed that one count, it's hard to tell what's going on with the rest of it. I agree with that.

I do think that it is still useful as a foil to what happened in this case. So if *Flyer* has a write blocker that is not properly applied and the court, in not granting the suppression, does note the dismissal is a factor in that decision. And I would say that what we have here is a different and, in some ways, more serious level of either

negligence or misconduct.

It is, frankly, mind-boggling to me that a federal agency that one of its primary tasks, as I understand it, of two is this electronic evidence, these cases like this. The Secret Service protects people, and it does cases of this nature.

Yet, when they put evidence in the Electronic Crimes Task Force vault, so the very people who are supposed to be experts on these things, they don't log in and out? And they don't even seem to admit that that is a concern or a mistake or that perhaps it should be done differently. And I think that's -- that sort of attitude about it is one of the things to consider when you're looking at what the purposes of suppression are.

So one purpose is to be fair to Mr. Seleznev. The other purpose is to deter this type of conduct. Because, without that type of deterrent, we're not seeing that anything here has shown anyone that they didn't handle it correctly or that it's not okay to do that.

Apparently, it's acceptable to take a laptop out of a vault, leave it in a workstation overnight, and just walk away. I find that extraordinary. Even on the level of very small counties and local law enforcement, there are protocols and established practices for what you do with the evidence and why you have an evidence room or a vault. We need to follow those. We need to follow them.

Because unless we all follow the same protocol, the reliability of the evidence that is supposedly stored by these people is in question. We can't just ignore that behavior and say, it's okay to -- just tell the jury they did that, and that makes it all better. Because it doesn't. We don't know what happened to this computer because they chose to mishandle it. I don't know if that's an individual agent decision. It appears to be -- in some ways, to be more of a training issue.

It is hard to understand the activation of the screen in the vault log. For one, it doesn't make any sense that they're looking for the serial number on July 9th, because they had the serial number on July 5th. They had the serial number on July 8th. And when they decided to go down the hall, they had to go from one vault to another in the same building on the same floor when they decided to do that. Apparently, that means they need to look for the serial number again. It turns on, and they just walk away. They just leave it there. We're just going to leave it in the vault turned on.

Now, we hear much later down the road, in the government's response, that that was a calculated decision. They left it on, because they were going to do a Live RAM Capturer. Mr. Carroll has explained to us exactly why, in his opinion, that makes sense. But the problem is, that doesn't appear to be

anywhere close to the rationale of the agents who made the decision.

Agent Mills testified, on cross-examination, that he thought of the Live RAM Capturer idea around the time that he obtained the test computer. So around the time of July 30th, not July 9th.

There's nothing in his notes that indicates on July 9th, we decided to leave it on so we could do a Live RAM Capturer. There's nothing in his reports that indicate that. There's nothing in Agent Fischlin's reports that indicate that that was the idea. The evidence the government points to for that being the idea all along is the email that Agent Mills sent on July 30th.

So it's left on. And we now know it's left on with a SIM card in it. We don't know who is going in and out of this room, because you only log in and out apparently at the beginning of the day and the end of the day. So who knows what's going on in the interim.

And then you take it out on July 30th, and it's off. Now, Agent Mills says it's off. Mr. Carroll says it is in a DRIPS state. Agent Mills is the one who saw it. He is a forensic examiner. I'm going to go with the thing is off, including this interesting issue about the unexpected-shutdown screenshot that Mr. Lahman had. So it showed that when you repower this drive, it shows that there was an unexpected

shutdown. The previous shutdown was unexpected on July 14th.

Mr. Carroll did an exhaustive amount of work on this case creating screenshots, going over government reports, being a helpful expert. It's very odd that he just decided not to run that test. He ran all of these other tests. We have all the stuff going on. He knows that this is what the defense experts are going to say, and he decides not to do it because the computer shut down on July 14th.

That's the point of that screenshot. You load the image. You power it up and it says it shut down. It's a very simple concept. The significance of that is that if it was shut down on the 14th and you don't see any file activity after that, July 30th, it makes no sense that you're plugging it in to do a Live RAM Capturer.

And Agent Mills acknowledges that. He testified that the reason for plugging it in for a change between Live RAM Capturer, something with a hex, and then there was another reason that had to do with imaging, traditional imaging. That that traditional imaging reason doesn't require you to plug it in.

So the computer is off, and then it is plugged in. Well, I think we can all understand that if a computer is plugged in, it's in a state of powered off. The splash screen is not going to activate when you just touch the thing on August 1st.

And then the level of file activity that we see on this computer doesn't support that the splash screen came on. We have a total of a million files. There are three files that randomly show up on this day. There's no event log changes. There is no registry key changes. All these things that we've been talking about for the last two days that are constantly changing and updating every time something happens.

So the significance of that piece is those -- so how are those files there? What is happening to this computer that that is showing up on August 1st? It's an example of why this drive is unreliable.

I do think it's interesting that Connected Standby has been around since 2008. Now, I understand that it was through this feature on Windows 8 where it was just already there was a fairly new thing, but, as a concept, it wasn't new. And these people are our experts in handling these things. We are not talking about the behavior of a normal detective or patrol officer on the street. We're talking about a specialized agent in electronic evidence. The idea that they know about BitLocker and everything else, but not Connected Standby is a difficult leap.

I'll conclude in saying that we can see the dangers of allowing this sort of thing to happen and what is in Agent Mills' report about the recent file items. And I'm not

saying that he -- purposely, he knew the access dates were different, but he put them in his report anyways.

What I'm saying is that he attributes things to a defendant in a criminal case. This person just accessed this. And this is significant to our investigation when, in fact, things aren't in that folder because of the access. And unless you have a case where the defense hires experts, no one is going to know that. And no one is going to know that, because all of these steps along the way where things weren't documented and mistakes were made and explanations were conjured along all of these steps, this behavior is not reported as part of the case.

The defense, I would indicate, got Agent Mills' notes at the end of January of 2016. In many, many cases, a defendant would have already resolved their case without anyone knowing about any of this. And so these things, when we spend all day looking at screenshots and file folders and logon behavior and all these things, they have a real-life consequence to the people who are charged with this type of offense.

And so I would ask that the court suppress this, because this isn't the type of behavior that should be condoned and allowed to go in front of a jury.

I have nothing further.

THE COURT: Thank you, counsel. Counsel for the

government?

GOVERNMENT'S CLOSING ARGUMENT

MR. BARBOSA: Thank you, Your Honor.

This is an unusual motion to suppress. Defendant is asking you to suppress the evidence entirely, but the evidence and testimony brought forth is the type of evidence and testimony you typically hear in a challenge to the weight of the evidence.

And issues like these, challenging the reliability of the evidence and the credibility of the witnesses, those are the types of factual determinations that we seat a jury for. That's what a jury typically hears. The evidence can go to the jury, as long as the government puts forth just a minimal showing that the evidence is reliable.

And there's case after case on the Ninth Circuit where evidence with many more questions about reliability goes to the jury, and the defense gets to present their challenge about its reliability and why they believe it shouldn't be trusted, and the jury decides.

To suppress evidence -- for the court to just completely suppress it and not even allow the jury to have the opportunity to look at it and test its reliability, the defendant has to prove that the government engaged in outrageous misconduct, not simple negligence or carelessness, but something outrageous. To meet that standard, they have

to show the agents intentionally acted in bad faith.

The defendant, as Ms. Scanlan just said, has raised two claims of bad faith. One, that the government engaged in illegal warrantless searches on July 7th. And, two, that they mishandled this computer throughout the time it was in their custody.

But the evidence they've produced to meet their burden fails to establish either of these allegations. What's worse is that it's not just that they have failed to bring forward sufficient evidence to prove that allegation, there is mountains of evidence that prove the exact opposite.

All of the reliable forensic artifacts show that this computer wasn't mishandled. And the last person to ever log on to the computer was the defendant shortly before he was captured in the Maldives. Nobody searched this computer before obtaining a warrant. The evidence proves that allegation is false.

First, before we even go into the forensic evidence, all of the logs and evidence that show there was no logon to this computer, there's the testimony of Agent Iacovetti at the airport in Guam waiting for his flight, at the same time that defendant claimed he illegally hacked into this computer.

This is an agent you've now heard from twice. You found him credible at the hearing on the defendant's motion to dismiss. And you heard from him that he was working for

several days on very little sleep. This was a whirlwind operation. He flew from Hawaii to Singapore to the Maldives to Guam. He was exhausted. He'd been working for five days.

The defense would have you believe that while sitting in the airport at the end of this gruelling trip, he pops this computer out of the bag, starts clicking around on the screen, guesses the password correctly despite not having any idea of what it is, and manages to completely erase all the logs which would have demonstrated these actions without a trace.

That may be one of the most absurd government conspiracy theories we've heard. Because to believe this, we'd have to believe that Agent Iacovetti, the guy who taped a bottle cap over the power button to keep it from lighting up -- this is an agent who led a massive government conspiracy to hack into the defendant's computer despite all the incriminating evidence.

That conspiracy theory just lacks any credibility. And one of the reasons it lacks any credibility is because the forensic evidence shows Agent Iacovetti is telling the truth. All of the forensic evidence shows that neither Agent Iacovetti or anyone else logged on to the computer after July 5th.

The security event log, Exhibit 29, shows the last user logon was July 4th at 4:07 UTC. The security event log,

Exhibit 17, shows the last user logoff was July 5th at 2:24:49 UTC. And the SRUM database, Exhibit 18, shows the last user-initiated activity on that computer was approximately 30 seconds before the last logoff. Totally consistent with Mr. Seleznev being the only one, the only human that used that computer before it was imaged.

But that's not all. The Windows update client, Exhibit 22, page 2, shows the last time the device was connected to a network was July 5th. Any network, wireless/cellular. Wireless, any network. The network registry, Exhibit 16, shows the last network it was connected to just happened to be the Kanifushi network, the name of his hotel he was staying at shortly before he was captured. And the network profile event log, Exhibit 14, showed that it disconnected from that network and connected to no others on July 5th.

All of these forensic artifacts, the forensic artifacts that are generally accepted in the computer-forensic community to establish these facts, show that no one logged on to this computer, remotely or directly.

So what has the defendant brought forward? They have brought forward two expert witnesses, paid expert witnesses who have offered theories that suggest all of this forensic evidence is false.

Defendant's conspiracy theory first rests on Mr. Lahman's misrepresentation of the Winlogon registry key. His

interpretation of that registry key is simply not credible, because he started with a conclusion somebody logged on to this computer. In examination of his testimony compared to the forensic evidence shows that what he did was selectively picked out forensic artifacts, took them out of context. He used those to bolster his conclusion, and he did it all without proper testing of his theories.

In the process, he simply tosses away all this evidence that shows he's wrong. He ignores event log after event log. Ignores the security event log, the application event log, the System Resource Use Monitor, and the USN journal log.

Instead, he bases his theory that someone logged on to a computer on a forensic artifact that has never been used before, and it's simply not an accepted basis in computer forensics for establishing a logon occurred.

And any artifact that doesn't support his theory, he attributes to inconsistent Windows behavior, but doesn't go back further to see if Windows behaves like that in other instances, which we've seen during Mr. Carroll's testimony that it does.

His theory that changes to the Winlogon registry key are caused by a logon is the premise of his entire report. He goes on about that. And for the rest of his report, the rest of his testimony, he premises everything on a user logged on, because the Winlogon registry key was changed. If this

premise is incorrect, everything else falls apart.

The only reason he believes the logs have been manipulated and a logon occurred is because he assumed that a Winlogon registry key change is an accurate indicator of a logon. But it isn't. He only tested that theory for a maximum of ten minutes. To test his theory of whether the Winlogon registry key might change under other circumstances, he didn't let the computer sit for 23 days. He didn't even let it sit for a full day. That is a basic failure of forensic science. We know it changes without user interaction.

Mr. Carroll conducted a more thorough test. In his test, it shows that the Winlogon registry key changes under several circumstances without a logon, at least these when the computer just sits unattended overnight, when the computer boots up and goes to the splash screen, and during any system repair function.

Mr. Blank's opinions are similarly based on false assumptions. He swears that all the post-seizure file access dates were the result of some form of user input. But just like Mr. Lahman's opinion, Mr. Blank's opinion is contradicted by all of the forensic evidence on the computer, all of the logs, all of the databases. All of the evidence on the computer shows nobody logged on to it, and no user was responsible for that behavior.

And the same evidence including, importantly, the System

Resource Use Monitor and the USN journal show exactly what did cause the changes to those files. Routine background activity, including the McAfee antivirus, Windows diagnostics, the Sony Vaio diagnostics, the SRUM database itself operating and monitoring the computer, and other routine systems that have nothing to do with agents hacking into his computer and planting evidence.

Mr. Blank also claims he can't dismiss the possibility of a remote logon, like some hacker just planted all of this stuff. And his concerns have grown exponentially, now that he's seen a SIM card exists. Even he admitted that a hacker remotely connected to this is unlikely. And in his report he didn't even discuss the fact that there were logs, numerous logs that showed this didn't happen. And those same logs would have recorded either a wireless or a cellular connection, and there's no evidence whatsoever to show that that occurred after July 5th.

Both Mr. Blank and Mr. Lahman claim the reason none of the evidence supports their theories is that someone could have manipulated the logs. That "someone" would have had to have been one of these government agents who testified, one of these government agents who the defense is claiming hacked into this computer and planted the evidence.

You heard from Mr. Carroll that, in an effort to cover up traces what Mr. Seleznev is claiming occurred, someone

logging on to the computer and planting hundreds of incriminating files, that would have left a trail a mile long. It would have been all over the computer. And he's never come across a hacker sophisticated enough to know how to cover up all of those traces, all of these logs that even some of these experts who have testified weren't aware of, weren't familiar with. This SRUM being a good example. Covering up those tracks would be almost impossible for all but the most-skilled hackers.

The only guy in custody of this laptop at the time defense claims the government hacked into it is Agent Iacovetti, the agent who taped the bottle cap over the power button.

This conspiracy theory is just not plausible. It is contradicted by the forensic evidence and the witness testimony. And for these reasons, it just cannot be found credible.

Defendant also claims that Agent Mills has lied to you, that he took the stand and he lied about seeing a splash screen on that computer on August 1st. You saw him testify. And you also heard from Mr. Carroll, who explained that he's reviewed the forensic evidence. And it's totally consistent with what Agent Mills found and what Agent Mills saw.

The three files that were created on August 1st show nothing different, show no mishandling of that computer. The defendant hasn't been able to prove outrageous conduct. They

haven't shown any agents engaged in any misconduct. They were trying their utmost best to do a very careful examination of this computer. They knew this was an important case. They went to the extraordinary lengths of getting a test computer and running multiple tests before imaging it. They tried to keep anything from happening to it.

This was agents doing their best, practicing forensic science as they had been trained in a rapidly-developing area. And as you heard in terms of the SIM card that was found today, it's something that they hadn't observed, something that the defense didn't see when they came over to examine the computer. But, nonetheless, there's no evidence that anybody logged on to that computer.

In terms of the staleness claim, the affidavit, Your Honor, I believe, establishes just overwhelming probable cause to believe that the computer would contain evidence not only of the defendant's ongoing criminal activity, but his history of online crimes over several years.

Mr. Browne repeatedly emphasizes the use of the term "may," with a concern that that is insufficient for probable cause. But probable cause doesn't require certainty, and the Supreme Court has said that. It doesn't even require a preponderance of the evidence.

The affidavit need only establish a fair probability that

evidence would be on defendant's computer. And a thorough review of that warrant shows the agent carefully went about establishing direct links between defendant's earlier credit card trafficking and hacking activity, using the "nCux," "Track2" and "Bulba," and the more recent and nearly identical credit card trafficking activity using the nic "2Pac."

The link between the defendant's Liberty Reserve accounts use of further Track2 and Bulba trafficking sites, and the newer Liberty Reserve accounts up through 2014 that were used to further the 2Pac trafficking site, those constituted direct evidence that the defendant was continuing to engage in the same types of crimes. And the affidavit established that the 2Pac site was active through July of 2014.

Mr. Seleznev's laptop was taken into custody the first week of July 2014. And the similar MO was a scheme the defendant was operating in 2009 through 2012 is further -- similar to the newer scheme in 2013, was further basis to believe that there was current probable cause.

And, finally, very telling, the fact that the administrator of 2Pac suddenly stopped posting updates to the site when the defendant was arrested was a strong indication that he was either running it or involved in the operation of that site. And with all that evidence, the totality of the circumstances establishes abundant and fresh probable cause.

That leaves us with an argument about the delay in obtaining the warrant. As you've seen, whether a delay in obtaining the warrant violates the Fourth Amendment is a fact-base inquiry that focuses on whether it was reasonable.

Well, let's think about this case. Isn't it an extraordinary case as evidenced by how long it's taken the prosecutor? This is the third full-day evidentiary hearing. We're heard testimony about an operation in the Maldives, the defendant's transport from the Maldives to Guam to here.

The case agent was, likewise, faced with extraordinary circumstances. He was brand new to the case. Back February of 2014 to July 2014 on an inactive investigation is clearly brand new.

This was a complex international investigation, several years old. The original investigators had moved on to other employment. The original AUSAs had retired. The new AUSA to the case was also brand new. And at the same time, the agent is working diligently trying to prepare an affidavit on a case he is unfamiliar with.

He had to also prepare for an identity hearing in Guam, which required him to dig through a very long file, and pulling exhibits, understanding how he was going to establish Mr. Seleznev's identity, and travel halfway around the world.

So faced with these extraordinary circumstances, he took extraordinary measures to move the warrant along. He

prepared the first draft within days of the arrest. He completed a second draft while he was in Guam distracted by multiple continuances of the hearing.

And this wasn't a simple five-page affidavit. Unlike some of the cases we've seen cited in the defense brief, this wasn't a drug warrant where the only probable cause was a dog sniffing a package. This affidavit was over 40-pages long. It contained extensive background expert testimony about how cyber criminals operated and numerous credit card trafficking, specific definitions. It also contained a great deal of expert testimony about electronic devices and how those searches are conducted. And the affidavit went through multiple sections describing a long and complicated electronic investigation.

Finally, when it became clear that the delay in Guam would prevent the agent from timely swearing out the affidavit after completing it, the agency had another agent fly from Washington, D.C., to swear out the warrant. These are agents acting with extreme diligence and doing everything they can to move the warrant along. And in light of those circumstances, the amount of delay was perfectly reasonable.

Your Honor, there are some things that forensic experts cannot explain on computers. As you heard from Mr. Lahman, they can't figure out certain things. Computers do unexpected things. Sometimes a computer just dies. Throws

out all the work you've been working on that decision that you wanted to get out this week, and we have no idea why. That doesn't mean we throw out everything on the computer. Computers can be a pain in the neck, but we know, from experience, that they are a reliable and useful tool in everyday life. And just like they are a reliable and useful tool in everyday life, they are a reliable and useful tool in recreating events.

Ms. Scanlan discussed evidence handling and was very critical of the agents' vault log procedures and Agent Mills' decision to have the computer on at his workstation in a secure Secret Service Electronic Crimes Lab.

Computers aren't like guns or drugs. They don't need to be handled in the same way, because they are essentially a recording device. And, as we've seen, they tell us what happened. This computer has told us what happened, and it tells us that nothing inappropriate happened. It tells us that these agents did not engage in any misconduct and the defendant's motion should be denied.

I have nothing further.

THE COURT: Anything further from the defense?

MR. BROWNE: Your Honor, I have nothing to add.

THE COURT: Ms. Scanlan?

MS. SCANLAN: I have nothing further.

THE COURT: Counsel, the court obviously is not going

to make a quick decision on this matter. I've heard two days of testimony. I'm going to go back and review my notes and make a conscience decision, based on my review of the argument and the facts that were presented.

So we need to set a date and time for the parties to return back to court. The best that I can give you, counsel, would be June 8 at 1:30. And I believe that the court dedicates -- certainly not tomorrow with the schedule I have. But some of this week and the beginning of next week, I should be able to give an in-court ruling on June 8th at 1:30.

Counsel for the government, any reason why you can't be present?

MR. BARBOSA: That's fine. Your Honor.

THE COURT: Counsel for the defense?

MR. BROWNE: Your Honor, I know I'm obligated. My cases are backing up all over the state literally on the 8th. But Ms. Scanlan is checking her phone now. She keeps her calendar on her phone and I keep mine in my head.

MS. SCANLAN: I left my phone in the room out there, so would you like me to check it now?

THE COURT: Check it now.

MS. SCANLAN: I'll be here.

THE COURT: Okay. Good. All right. Counsel, the return date will be June 8th, at 1:30, in this courtroom.

We'll be in recess until then.

(PROCEEDINGS ADJOURNED.)

C E R T I F I C A T E

I, Nancy L. Bauer, CCR, RPR, Court Reporter for the United States District Court in the Western District of Washington at Seattle, do hereby certify that I was present in court during the foregoing matter and reported said proceedings stenographically.

I further certify that thereafter, I have caused said stenographic notes to be transcribed under my direction and that the foregoing pages are a true and accurate transcription to the best of my ability.

Dated this 2nd day of August 2016.

/S/ Nancy L. Bauer

Nancy L. Bauer, CCR, RPR
Official Court Reporter